Users Guide

Wyse® Winterm™ 1 series, Based on Wyse Thin OS

Issue: 121906
PN: 883681-08 Rev. E

WYSE

Copyright Notices

End User License Agreement (“License”)

A copy of the Wyse Technology End User License Agreement is included in the software and provided for your reference only. The License at http://www.wyse.com/license as of the purchase date is the controlling licensing agreement. By copying, using, or installing the software or the product, you agree to be bound by those terms.

Trademarks

Wyse and Winterm are registered trademarks, and the Wyse logo and Winterm logo are trademarks of Wyse Technology Inc. ICA is a registered trademark and MetaFrame is a trademark of Citrix Systems Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation. All other products are trademarks and/or registered trademarks of their respective companies. Specifications subject to change without notice.

Patents

This product and/or associated software are protected by copyright, international treaties, and various patents, including the following U.S. patents: 6,836,885 and 5,918,039.

Restricted Rights Legend

You acknowledge that the Software is of U.S. origin. You agree to comply with all applicable international and national laws that apply to the Software, including the U.S. Export Administration Regulations, as well as end-user, end-use and country destination restrictions issued by U.S. and other governments. For additional information on exporting the Software, see http://www.microsoft.com/exporting.

Ordering Information

For availability, pricing, and ordering information in the United States and Canada, call 1-800-GET-WYSE (1-800-438-9973) or visit us at http://www.wyse.com. In all other countries, contact your sales representative.

FCC Statement

This equipment has been tested and found to comply with the limits for either Class A or Class B digital devices (refer to “Thin Client Requirements Compliance”), pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution

Changes or modifications not covered in this manual must be approved in writing by the manufacturer’s Regulatory Engineering department. Changes or modifications made without written approval may void the user’s authority to operate the equipment.

Thin Client Requirements Compliance

FCC Compliance

Model SX0, Product S10 thin clients meet Class B requirements.

IEC/EN Compliance

Model SX0, Product S10 thin clients meet Class B requirements.

Canadian DOC Notices

Refer to the previous section, "Thin Client Requirements Compliance," to find out to which model thin client each of the statements below refers.

Class A - This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Réglement sur le brouillage radioélectrique édicté par le Ministère des Communications du Canada.

Class B - This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe B prescrites dans le Réglement sur le brouillage radioélectrique édicté par le Ministère des Communications du Canada.

IEC/EN Notice

This product conforms to the requirements of IEC950 and EN60950.

This product conforms to requirements of EN55022 for Class A equipment or EN55022 for Class B equipment (refer to "Thin Client Requirements Compliance").

Cable Notice

The use of shielded I/O cables is required when connecting this equipment to any and all optional peripheral or host devices. Failure to do so may cause interference and violate FCC and international regulations for electromagnetic interference.

Noise Suppressor

A noise suppressor (ferrite bead) must be installed on the network cable of your thin client (except Model SX0). This installation is necessary to maintain compliance with U.S. FCC B limits and European CISPR B EN55022 Class B limits. The noise suppressor is supplied by the manufacturer and is packed in your thin client shipping carton.

Device Power Supply

For use with external power supply included in the shipping carton, or a certified equivalent model supplied by the manufacturer.

Model SX0, Product S10 Thin Client

For use with External Power Supply DVE Model DSA-0421S-12 3 30 or certified equivalent model supplied by the manufacturer, rated minimum 12Vdc, 2.5A.

This page intentionally blank.

Contents

1 Introduction

Wyse® Winterm™ 1 series Thin Clients use Wyse Thin OS. These highly optimized thin clients provide ultra-fast access to applications, files, and network resources made available on machines hosting Citrix™ ICA and Microsoft™ RDP session services. Locally installed software permits remote administration of the thin clients and provides local maintenance functions.

Session and network services available on enterprise networks may be accessed through a direct intranet connection, a dial-up server, or an ISP which provides access to the Internet and thus permits the thin client to connect to an enterprise VPN (virtual private network) server.

About this Guide

This guide is intended for users of the Wyse® Winterm™ 1 series Thin Client. It provides detailed instructions on using the thin client to manage the connections and applications available to users from a network server.

Organization of this Guide

This guide is organized as follows:

Chapter 2, "Getting Started," provides information to help you quickly get started using your thin client. It describes basic thin client functions and provides instructions on using the Desktop and Connect Manger to manage the connections and applications available for you to use.

Chapter 3, "Setting Up the Thin Client," contains information to help you set up your thin client using the System Setup submenu.

Chapter 4, "Using and Configuring Access Connections," provides information and detailed instructions on using and configuring connections to access the enterprise server environment available to the thin client.

Chapter 5, "Using the Network Test Tools," contains information on using the Network test tools available on the thin client.

Wyse Technical Support

To access Wyse technical resources, visit AskWyse.com. If you still have questions, you can submit your questions using the Wyse Support Request Form, or call Customer Support at 1-800-800-WYSE (toll free in U.S. and Canada). Hours of operation are from 5:00 am to 5:00 pm PST, Monday through Friday.

To access international support, visit http://www.wyse.com/global.

Related Online Resources Available at Wyse

Wyse® Winterm™ 1 series Thin Client features can found in the Datasheet for your specific thin client model. Datasheets are available on the Wyse Web site at: http://www.wyse.com/serviceandsupport/support/documentindex.asp.

The *Administrators Guide*: *Wyse® Winterm™ 1 series, Based on Wyse Thin OS* is intended for administrators of the Wyse® Winterm™ 1 series Thin Client. It provides information and detailed system configurations to help administrators design and manage a Wyse® Winterm™ 1 series Thin Client environment. It is available at: http://www.wyse.com/manuals.

2 Getting Started

This chapter provides information to help you quickly get started using your thin client. It describes basic thin client functions and provides instructions on using the Desktop and Connect Manger to manage the connections and applications available for you to use.

What Happens When You Turn on Your Thin Client

What you see, initially, when you turn on or reboot your thin client, depends on your method of access to the enterprise intranet and how your network administrator has set up your account. With Wyse Thin OS software, your thin client can also be turned on by the Wake-On-LAN feature. Using this feature, an administrator can turn on the thin client connection by using a LAN message that the thin client recognizes on a single Ethernet subnet.

Accessing the Enterprise Servers Available

There are five basic methods of access to the enterprise server environment available to the thin client. Except for Ethernet Direct, all of the access methods require that some local settings be made on the thin client. These settings cannot be automated because the thin client has not yet accessed Global and User profiles. For certain privileges, these local settings are retained and are available for the next thin client system start. Activating these local settings and the defined connections can also be automated at thin client system start.

Methods of access include:

- **Ethernet Direct** - This is a connection from the thin client Ethernet port directly to the enterprise intranet. No additional hardware is required. An account sign-on dialog box displays if required, then either the desktop or an application window opens (the application window opens, with or without a session server logon requirement, if set by the administrator to open automatically). User profiles normally are used in this mode and are accessed automatically. However, if the Dynamic Host Configuration Protocol (DHCP) - a protocol for assigning dynamic IP addresses to devices on a network - is not available on the enterprise intranet, the location of the file server where user profiles are located must be entered in the Network Setup dialog box. For information on the Network Setup dialog box, refer to "Configuring Network Settings."
- **Wireless Direct** - If a wireless network device is connected to the thin client but a wireless connection has not yet been configured, the Wireless Setup dialog box opens. When a connection is established, the behavior is the same as for an Ethernet Direct connection, including automatic access to user profiles through DHCP. For information on the Wireless Setup dialog box, refer to "Setting Up Wireless Access."
- **PPPoE** - The PPPoE Manager dialog box is available from the desktop to configure and invoke PPPoE connection to WAN. Once connected, all WAN packets go though a PPP connection over Ethernet to the DSL modem. The PPPoE Manager is not accessible for users with sign-on privilege set to None. Open the PPPoE Manager

dialog box by selecting it from the desktop menu. This dialog box also can be set to open automatically on system start-up. For information on the PPPoE Manager dialog box, refer to "Configuring PPPoE Access."

- **Dialup Modem** - If both the Dialup Manager and the Connect Manager open automatically when the thin client is turned on or restarted, the thin client is configured to access the network through a modem dial-up. A sign-on dialog box may appear when the network connection is accomplished. DHCP cannot automatically connect your thin client to User profiles when using dial-up access; the location of the FTP server where the profiles reside must be entered in the Network Setup dialog box. For information on the Dialup Manager dialog box, refer to "Configuring Dialup Modem Access." For information on the Connect Manager, refer to "Using the Connect Manager." For information on the Network Setup dialog box, refer to "Configuring Network Settings."
- **PPTP VPN** - The PPTP Manager dialog box can be configured to open automatically when the thin client is turned on or restarted. This facilitates connection to an enterprise network through an ISP, the Internet, and a virtual private network (VPN) PPTP server. If dial-up is used to contact the ISP providing access to the Internet, the Dialup Manager and Connect Manager also open. DHCP cannot automatically connect your thin client to User profiles when using PPTP VPN access; the location of the FTP server where the profiles reside must be entered in the Network Setup dialog box. For information on the PPTP Manager dialog box, refer to "Configuring PPTP VPN Access." For information on the Dialup Manager dialog box, refer to "Configuring Dialup Modem Access." For information on the Connect Manager, refer to "Using the Connect Manager." For information on the Network Setup dialog box, refer to "Configuring Network Settings."

Note

If the Network Setup dialog box initially appears, or the Connect Manager is active when the thin client is started (or when the enterprise intranet is accessed), network services are not fully configured. In this case sign-on is not required and thin client network settings (and possibly connection definitions) must be entered locally on the thin client (for example, a Stand-alone user). For more information, refer to “Using the Connect Manager” and "Configuring Network Settings."

If the network to which the thin client is connected does not provide FTP services, a User profile will not be available and network addresses and connection definitions must be entered locally on the thin client. If User profiles (and update services) are available from an FTP server but DHCP does not supply the location of the FTP server, you can access the profiles by entering the location of the FTP server locally on the thin client (refer to “Configuring Network Settings” for more details).

Signing-on

After a connection to the enterprise intranet is established, sign-on to the network and/or session services may or may not be required (depending on a Global profile option set by the network administrator, the session servers, or any requirements of PNAgent/PNLite services). If sign-on to the enterprise intranet is required, a sign-on dialog box opens when you turn on the thin client, when you restart the thin client, or after signing off from a User profile account.

Note

In a Virtual Desktop environment, user authentication is made against the Virtual Desktop Broker. Therefore, you will only authenticate against the Broker. You will sign-on as described in this section only when a Virtual Desktop environment is not used or is unavailable.

Sign-on name and password are assigned initially by the administrator when the account is established, but the password can be changed by the user at a thin client in some cases (see "Changing Your Password"). To sign on to a standard account, enter the user name for the account and password allocated to you by the network administrator. Account user names are not case sensitive, however, passwords are case sensitive.

Note

If you cannot successfully sign-on, ask your network administrator for help.

If a user account is not established but PNAgent/PNLite-published applications are to be accessed on the PNAgent/PNLite server, you must enter the user name for the account and password (in this case, account user names are not case sensitive, but passwords are case sensitive) and also select a Domain in which the applications appears (if the correct domain does not appear in the list, type it into the Domain box).

Note

Applications can be published to the network by PNAgent/PNLite services. These applications are available to the thin clients on the network as long as accounts are established on the PNAgent/PNLite server. If User profiles are used, the thin client will send the enterprise server sign-on and domain information to the PNAgent/PNLite server for log-on. If User profiles are not used (a sign-on is not required to access User profiles) but a PNAgent/PNLite server address is entered into the Network Setup dialog box, the sign-on dialog box with the PNAgent/PNLite Domain box will still be presented to you for access to the published applications. PNAgent/PNLite-published applications will be merged with connections defined through user profiles and local settings for a combined total number of connections. The maximum number of connections has a default limit of 216, but can be set from 100 to 1000 through wnos.ini.

Changing Your Password

If you are required to sign on and you are not using PNAgent/PNLite services or a Virtual Desktop environment, you can change your assigned password by selecting **Check here to change password** in the sign-on dialog box and using the change password dialog box (type the new password in both the New Password and Confirm boxes, and click **OK**).

Note

If you are using both PNAgent/PNLite and a User profile, the user name must be defined in the Windows domain to be used and the password must be the same for both the domain and the User profile.
In a Virtual Desktop environment, user authentication is made against the Virtual Desktop Broker (the user name and password are stored on the Broker or a third party authentication server). Therefore, the password must be changed on the Broker or the authentication server.

If you are required to sign on and are using PNAgent/PNLite services (so that the user profile password is forwarded to the PNAgent/PNLite server), you can have an application change your domain password but you cannot change your ini file password while using PNAgent/PNLite. Therefore, if you change the domain password, you will lose the effect of any directives in the user ini file, including any potential upgrade of privilege (for example, the privileges in the wnos.ini file may be set to None, but the privileges in the user ini file are set to High).

Understanding Your User Profile

Profiles for users contain the settings and connection definitions for the thin client. They are created and maintained by the network administrator and reside on the enterprise intranet FTP server or Virtual Desktop server. The thin client accesses these user profiles when you sign on. The location of these files may be automatically supplied to the thin client by the DHCP server (if set up by the network administrator), or if DHCP is not available, their location must be entered in the Network Setup dialog box.

Note

The Global profile (wnos.ini) and User profile (user.ini) on an FTP server can take effect only when a Virtual Desktop environment is not used.

Types of user profiles include:

- **Global** - All clients of the same FTP server have these profile settings.
- **User** - Only the individual user has these profile settings. Settings in User profiles can override corresponding Global profile settings.

Note

If you want to change your user profile, ask your network administrator.
In a Virtual Desktop environment, the user profile is set in the user policy. Therefore, different users with the same policy will have the same user profile.

You have the same user profile, regardless of which thin client you use. If allowed by the network administrator, a limited number of settings are available locally. For instructions on selecting local operator preferences such as display, keyboard, mouse, and printer selections, refer to "Setting Up the Thin Client."

Note

If the network to which the thin client is connected does not provide FTP or Virtual Desktop services, a user profile will not be available and network addresses and connection definitions must be entered locally on the thin client. If user profiles are available from an FTP or Virtual Desktop server but DHCP does not supply the location of the server, you can access the user profiles by entering the location of the FTP or Virtual Desktop server locally at the thin client (refer to "Configuring Network Settings" for more details).

Knowing Your Assigned Privileges and User Mode

As a thin client operator, you have a thin client account with certain privileges. Your thin client account is a set of application connection definitions and thin client configuration settings that are grouped under a privilege level and assigned to you by your administrator. Administrators create thin client accounts that possess specific connection capabilities, security, and various thin client functions. Assigned privileges and user modes allow you certain levels of access to thin client resources.

Note

User access to system-reset-to-factory defaults and the Network Setup dialog box can be denied by the user privilege (not the lock-down state). Therefore, if the thin client is locked down in High privilege, you will have access to all facilities, regardless of other items (unless there is an intervening privilege statement in an ini file). It is only when the thin client is locked down in the privilege None that you cannot recover control of the thin client. For more information about system lock-down, refer to "Understanding System Lock-down."

Assigned Privileges

The user profiles (Global and User) can assign three privilege levels of access to thin client resources: High-privileged, Low-privileged, and Non-privileged.

- **High-privileged** - With High privilege, all thin client resources are available with no restrictions. This is an administrative level of log-on. Connection definitions can be entered locally on the thin client, but they will typically be lost upon log-off/shutdown of the thin client. However, if configured by an administrator (`enablelocal=yes`), locally-defined connection definitions can be saved. If you are a user at this level, you can reset the device to factory defaults.

Note

High privilege is the default privilege (unless locked down in another privilege) and is in effect if a user profile is read that does not contain a privilege statement. If no wnos.ini file is read (same conditions), the connection definitions entered locally on the thin client are persistent and may even be visible if a wnos.ini file is found on a subsequent reboot (if an `enablelocal=yes` statement is read from one of the ini files).

- **Low-privileged** - This is the level assigned to a typical user of the thin client. The Network and Wireless selection on the System Setup submenu is disabled (the Network Setup dialog box and Wireless Setup dialog box cannot be opened). A Low-privileged user cannot reset the device to factory defaults.
- **Non-privileged** - This level of access is typical for kiosk or other restricted-use deployment. The System Setup selection on the desktop menu is disabled (the various dialog boxes available from the System Setup cannot be displayed). The Connect Manager is not available. The user cannot reset the device to factory defaults. Both the Dialup Manager and PPTP Manager dialog boxes are disabled.

Note

If you are accessing the enterprise intranet through Dial-up or PPTP VPN, the Network Setup dialog box is available during the dial-up process to establish the initial connection to the FTP server. If you then log on as a Low-privileged or Non-privileged user, however, access to the Network Setup dialog box is then disabled. The Dialup Manager and PPTP Manager dialog boxes are also disabled for a Non-privileged user.

User Modes

User Modes define your login state and include the following types of user:

- **Guest user** - The Guest user mode logs on using the Global profile only (no User profile is available) and does not need a password. But the Guest user will be disabled if no connection is defined in the Global profile. The Guest user cannot access the Network Setup dialog box and cannot reset the device to factory defaults. Otherwise, all remaining local resources are available. Although an enterprise file services account password is not required, individual application servers may require a password.
- **Stand-alone user** - This mode makes operation of the thin client possible when user profiles or PNAgent/PNLite-published applications are not available. No user log-on is required and network information and connection definitions must be defined locally on the thin client. Locally entered connection definitions are preserved when the thin client is turned off or restarted, but individual user accounts are not available and automatic software updates are not available when the thin client is restarted.

Note

It is possible to have an FTP server which supplies software updates but no .ini files. In this case, software updates would take place but the user would still be Stand-alone.

- **PNAgent/PNLite-only user** - This mode is similar to a Stand-alone user, except applications published by Citrix PNAgent/PNLite services are available (the IP address of a PNAgent/PNLite server is entered into the Network Setup dialog box). The user logs on to the PNAgent/PNLite server but does not log on to the file server or use configuration user profiles. If the PNAgent/PNLite server publishes fewer than the limit of applications set by the administrator, the user can locally define additional applications. As long as the domain password for the PNAgent/PNLite server matches the password in an ini file for the same user on the FTP server, both the PNAgent/PNLite published applications and the directives in the user ini file will be processed (with the PNAgent/PNLite published applications being processed first). However, other directives from the user ini file could alter the privilege, the default display resolution, and so on. With the enable local clause for the connect statement, connections defined in the user ini file may be persistent.

Understanding System Lock-down

Your administrator can configure whether or not to allow access to the Network Setup dialog box to locally re-configured the thin client to operate in a different mode or to access a different file server.

Note

High-privileged users always have access to the Network Setup dialog box.

During normal thin client operation, Low-privileged and Non-privileged users may access the Network Setup dialog box by temporarily disconnecting the Ethernet cable from the rear of the thin client and rebooting to Stand-alone user mode. The Network Setup dialog box can also be accessed by a hot-key reset to factory default, in addition to the system reset available to a Stand-alone user through the Sign-off/Shutdown/Shutdown and Restart the system dialog box.

In most cases, access to normal operation resources is desirable. However, network environments requiring maximum security typically do not permit uncontrolled changes to thin client network operation. To achieve this security, the network administrator can place a lock-down argument in any privilege statement (either in the user .ini file or in wnos.ini

file). This prevents Low-privileged and Non-privileged users from accessing the Network Setup dialog box by resetting the thin client or through system restart to Stand-alone user mode.

Caution

If a thin client accesses the enterprise intranet through Dial-up or PPTP and the thin client is locked-down, a user attempting to reboot to Stand-alone user mode will disable the Network Setup dialog box. The user will not be able to re-access the enterprise intranet through this path. If this happens, the thin client must be moved to a location where it can access the intranet directly so that an administrator can set the profile to unlock the thin client. If the thin client is configured for Dial-up access, there must be an RAS server answering the configured telephone number. Otherwise, the thin client will require factory attention for recovery.

About the Session Services You Will Use

The Desktop connection icons and Connect Manager list entries allow you to initiate connections to servers providing ICA and RDP services. These services are configured by the administrator for you to use. Depending on your privileges you can modify some of the settings on these services. You can start connections by using the various Desktop or the Connect Manager options made available by the administrator.

The Multiple Sessions feature allows the thin client to have multiple active connections. The number of active connections you can have depends on the following:

- amount of RAM
- types of connections open
- number of connections configured

For more information on ICA connections, refer to "Configuring ICA Connections."

For more information on RDP connections, refer to "Configuring RDP Connections."

Logging Off and Shutting Down

After using your thin client, you can sign off from your account (if you signed in initially) or you can shut down the thin client (if your privilege or user mode allows you to do this).

Note

High-privileged, Non-privileged, and Guest users can also sign off from the Connect Manager.

Click the Desktop User Name button on the taskbar and select **Shutdown** from the Desktop menu to open the Sign-off/Shutdown/Shutdown and Restart the system dialog box. Use this dialog box to do one of the following:

- **Sign-off from the account User Name** - Allows you to sign off from the current open account (the sign-on dialog box appears and is ready for another user).
- **Shutdown the system** - Turns off the thin client.
- **Shutdown and Restart the system** - Signs off the user account and also allows posted software updates to be loaded into the thin client memory (the sign-on dialog box appears after the thin client restarts).
- **Restart the system setting to factory default** - Appears for High-privileged and Stand-alone users only. This option allows you to reset the thin client to factory defaults.

Note

Depending on how the servers and applications are configured, signing off from or shutting down the thin client may not necessarily close/open server sessions. Generally, you should close sessions before signing-off from or shutting down the thin client.

Using the Desktop

The desktop has a plain background with a horizontal taskbar at the bottom of the screen. The number of icons that can be displayed on the desktop depends on the desktop resolution and administrator configuration.

Note

Custom icons can be assigned to any or all connections defined in the ini files or a default icon can be used. If no icon is assigned to a connection, the connection will only appear in the Connect Manager and not on the desktop. Connections supplied by PNLite and PNAgent have icons assigned by the server. If you have a High privilege level, you can right-click an icon to open a Connections Settings dialog box.

If configured by your administrator (`Longapplicationname=yes` as defined in wnos.ini), the number of icons displayed for a resolution is as follows:

- 640 x 480: Up to 8 icons are displayed.
- 800 x 600: Up to 10 icons are displayed.
- 1024 x 768: Up to 21 icons are displayed.
- 1280 x 1024: Up to 40 icons are displayed.
- 1600 x 1200: Up to 60 icons are displayed.

PNAgent - The thin client features PNAgent (a Program Neighborhood folder support). With PNAgent, icons are populated to folders based on the Program Neighborhood setup on the server. Depending on the Citrix server configuration, these icons can display on the desktop, in the Desktop menu, in the Connect Manager, and in the system tray.

Note

If any network connection is designated to open automatically on startup, it will open and you will see the server log-in or server application window instead of the desktop.

Figure 1 Desktop example

Use the following guidelines:

- Icons representing available server connections and published applications are displayed on the background. Hovering the mouse pointer over an icon pops-up information about the connection. Right-clicking (or left-clicking if the mouse buttons are reversed) on an icon opens a **Connection Settings** dialog box which displays additional information about the connection.
- You can open a server connection/published application by double-clicking a desktop icon or you can navigate to the desktop icon you want by using tab key and pressing **Enter** to initiate the connection.
- The desktop menu may be opened by clicking the mouse button on the desktop background or by clicking on the User Name button on the task bar.
- If configured to display (by an administrator), the volume control is displayed in the right corner of the taskbar and the current time and date are shown when the cursor is placed on the time.

Note

The thin client is capable of synchronizing its clock to time provided by a Simple Network Time Protocol (SNTP) server.

- Use CTRL+ALT+UPARROW to toggle between window display modes.
- Use CTRL+ALT+DOWNARROW to open a selection box for toggling between the desktop, Connect Manager, and currently-active connections.
- Keyboard shortcuts are supported. Use the LEFT ALT+UDERLINED LETTER on the keyboard for keyboard shortcuts (the RIGHT ALT+UDERLINED LETTER combination is not currently supported).
- Use the System Preference dialog box to switch the left and right buttons. For information on the System Preference dialog box, refer to "Setting System Preferences."
- In addition to the standard two-button mouse, the thin client supports a Microsoft Wheel Mouse (used for scrolling). Other similar types of a wheel mouse may or may not work.
- You can copy and paste between application sessions and between sessions and the desktop, however, this function depends on session server configurations.

Viewing System Information

System information is available from the taskbar and from the System Information dialog box.

If configured by the administrator, CPU usage and free memory are displayed in the box on the right side of the taskbar. If you click on this area, it will toggle between percent of CPU usage currently in use and available free memory in megabytes. If you put the mouse cursor on the taskbar without clicking, a popup appears showing the number (for example, percent of CPU currently in use and available free memory in megabytes). This information is also available in the System Information dialog box.

Note

Starting an ICA or RDP connection requires at least 2 megabytes of free memory.

Clicking the ? icon on the task bar (or selecting **System Information** from the Desktop menu) opens the System Information dialog box where you can view thin client system information (see "Accessing System Information").

Understanding the Window Display Modes

The thin clients allow three different display modes, including:

- **Standard window** - Window frame, title bar, content area, including icons, and so on. This mode is available for use with any connection.
- **Seamless window** - Seamless display. This mode is available for use with published applications only.
- **Full-screen** - Occupies the entire monitor screen with no thin client taskbar, title bar, or window borders. This mode is available for use with any connection.

Note

In all display modes, use CTRL+ALT+DOWNARROW to open a selection box for toggling between the desktop, Connect Manager, and currently-active connections.

The display modes that are available depend on what window mode was in use when the connection was started. That in turn depends on the relative resolution settings of the screen and connection. The screen resolution is the actual hardware resolution used by the thin client video chip (local resolution set either by DDC or selected manually and is referred to as the default resolution). This resolution can be different than the connection resolution (set with the Connection Settings dialog box or in the user profile by the administrator), which is the dimensions of the connection screen display in pixels.

Use the following guidelines:

- If the connection is started in full-screen mode, a user can toggle between Full-screen mode and Standard window mode by using CTRL+ALT+UPARROW.
- If the connection is started with either the default resolution or a connection resolution matching the current display resolution, *and* then the Seamless window mode is selected, the connection starts in the Seamless window mode (the Seamless mode has a few less rows of pixels than the Full-screen mode to make room for the thin client task bar at the bottom of the screen). The task bar displays on startup, but can be modified to be shown or hidden by using CTRL+ALT+UPARROW. In this Seamless window mode the connection display cannot be moved to a different location on the screen, regardless of whether or not the task bar is displayed. When the task bar is hidden, the area at the bottom of the screen is blank (black). When the task bar is shown, it can be used to switch between sessions simply by clicking an icon for another session in the task bar.
- If the connection is started with an explicit resolution (that is, something other than the default resolution set in the user profile or Connection Settings dialog box) less than the current default resolution and the Standard window mode is selected (in the Connection Settings dialog box or in the user profile setting), the connection is displayed in a Standard window. Using CTRL+ALT+UPARROW changes the current screen resolution to match the connection resolution and the connection is displayed in Full-screen mode. Using CTRL+ALT+UPARROW again restores the original screen resolution and will again display the connection in the Standard window mode. In Full-screen mode the hardware resolution changes only for the duration of the connection, then changes back to the default resolution when the connection is no longer in the foreground.
- Making a Seamless window a Full-screen display does not cause the application to fill the screen. Instead, the application remains the same size and any portion of the screen previously not occupied is filled with a black mask (including the screen space previously occupied by the thin client taskbar).

Note

The thin client features PNAgent (a Program Neighborhood folder support). With PNAgent, icons are populated to folders based on the Program

Neighborhood setup on the server. These icons display on the desktop and in various places (for example, Systray and the user Desktop submenu application selections) depending on the Citrix server configuration.

For more information on configuring the resolution and refresh rate for the monitor used with the thin client, refer to "Selecting Display Settings."

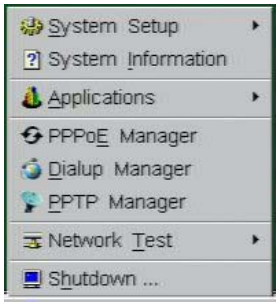
Using the Shortcut Menu and Desktop Menu

Right-clicking on the desktop provides a Shortcut menu with the following options:

- **Hide all windows** – To bring the full desktop to the foreground.
- **Copy to clipboard** – To copy the image of the full screen, current window, or event log to the clipboard. The clipboard contents can then be pasted to an ICA or an RDP session.
- **Purge clipboard** – To discard the contents of the clipboard in order to free up memory.
- **Lock Terminal** – To put the terminal in a locked state if the user has signed on to the system with a password. The terminal can only be unlocked using the same password.

Clicking the User Name desktop button on the task bar opens the Desktop menu (the Desktop button shows the user log-on name).

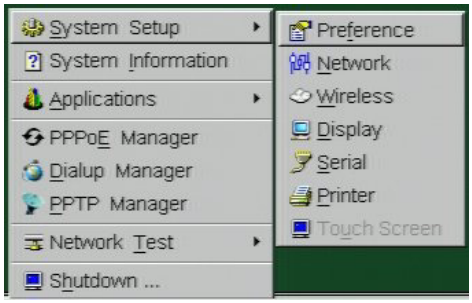
Figure 2 Desktop menu



Using the System Setup Submenu

Selecting **System Setup** in the Desktop menu opens the System Setup submenu (for High-privileged and Low-privileged users only).

Figure 3 System Setup Submenu



The System Setup submenu provides access to the following local system setup dialog boxes:

- **Preference** - Allows user selection of thin client parameters that are a matter of personal preference. For more information on the System Preference dialog box, refer to "Setting System Preferences."
- **Network** - Facilitates selection of DHCP or manual entry of network settings, operation in modem dialup and PPPoE modes, as well as entry of locations of servers essential to thin client operation. This menu selection is disabled for Low-privileged users. For more information on the Network Setup dialog box, refer to "Configuring Network Settings."
- **Wireless** - Allows entry of parameters required for wireless wide-band modem access to the enterprise intranet. For more information on the Wireless Setup dialog box, refer to "Setting Up Wireless Access."
- **Display** - Facilitates selection of the desired resolution and refresh rate for the monitor used with the thin client. For more information on the Display Setup dialog box, refer to "Selecting Display Settings."
- **Serial** - Facilitates configuration of the ports for modem dialup mode and serial communications. For more information on the Serial Setup dialog box, refer to "Configuring Serial Communications."
- **Printer** - Allows configuration of network printers and local printers that are connected to the thin client. For more information on the Printer Setup dialog box, refer to "Setting Up Printers."
- **Touch Screen** - Allows configuration of Serial and USB touch screens from ELO, MicroTouch (Model M150 only), or FastPoint. For more information on Touch Screen setup, refer to "Configuring Touch Screens."

Accessing System Information

Selecting **System Information** in the Desktop menu opens the System Information dialog box.

The following information is available:

- **General Tab -** Displays general information such as System Version, Serial Number, Boot From, Memory Size (Total and Free), Terminal Name, IP Address, Net Mask, Gateway, and DHCP Lease.
- **Devices Tab -** Displays information about devices such as the CPU Speed, ROM Size, Monitor, Parallel Ports, Ethernet Speed, Memory Speed, NAND Size, Resolution, Serial Ports, and the thin client MAC Address.
- **Copyright/Patents Tab** - Displays the software copyright and patent notices.
- **Event Log Tab -** Displays the thin client start-up steps (normally beginning from System Version to Checking Firmware) or error Messages that are helpful for debugging problems.
- **Status Tab -** Displays status information about TCP performance-related parameters, CPU Busy, System Up Time, Wireless performance-related parameters, Free Memory, and DHCP lease time remaining.

Accessing Available Applications

Applications is an additional desktop menu option that is available. Applications contains a submenu of all locally configured applications and is populated with published applications when a user is signed on using either PNLite or PNAgent.

Accessing the PPPoE Manager

Selecting **PPPoE Manager** in the Desktop menu opens the PPPoE Manager dialog box. Use this dialog box to configure or start PPP connection over Ethernet to a DSL modem. The terminal can be configured to run PPPoE to connect to WANs through DSL modems to eliminate the need of installing a DSL router between the terminal and the DSL modem. You can also use this dialog box to automatically open a connection on system start-up.

For more information on the PPPoE Manager dialog box, refer to "Configuring PPPoE Access."

Accessing the Dialup Manager

Selecting **Dialup Manager** in the Desktop menu opens the Dialup Manager dialog box. Use this dialog box to initiate a connection through a modem. This dialog box also opens automatically on log-on when a thin client is configured to access a network through a modem and a dial-up server.

For more information on the Dialup Manager dialog box, refer to "Configuring Dialup Modem Access."

Note

The Dialup Manager dialog box is not available to Non-privileged users.

Accessing the PPTP Manager

Selecting **PPTP Manager** in the Desktop menu opens the PPTP Manager dialog box. Use this dialog box to initiate a connection through an enterprise Virtual Private Network (VPN) via an Internet Service Provider (ISP), the Internet, or a PPTP VPN server. This dialog box can also be set to open automatically on system start-up.

For more information on the PPTP Manager dialog box, refer to "Configuring PPTP VPN Access."

Note

The **PPTP Manager** dialog box is not available to Non-privileged users.

Accessing the Network Test Tools

Selecting **Network Test** in the Desktop menu opens a submenu from which the Ping and Trace Route dialog boxes can be opened. Use the Ping and Trace Route dialog boxes to check the integrity of the network connection.

For more information on the Ping dialog box, refer to "Using Ping."

For more information on the Trace Route dialog box, refer to "Using Trace Route."

Accessing the Shutdown Options

Selecting **Shutdown** in the Desktop menu opens the Sign-off/Shutdown/Shutdown and Restart the system dialog box. Use this dialog box as described in "Logging Off and Shutting Down."

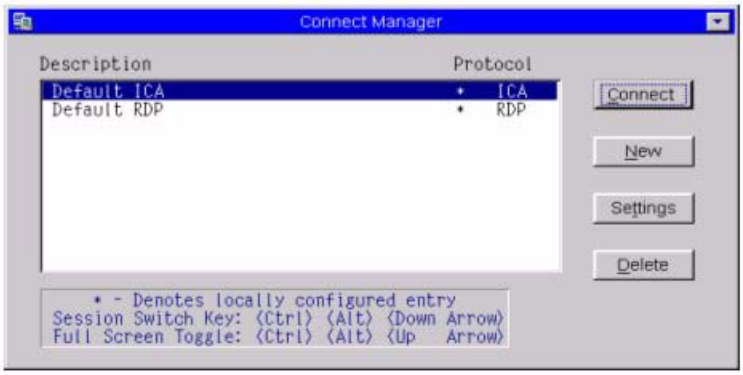
Using the Connect Manager

Clicking the Connect Manager button on the task bar opens the Connect Manager. The Connect Manager has a list of connection entries and a set of command buttons available for use with the connections.

Note

Non-privilege users cannot view the Connect Manager.

Figure 4 Connect Manager (High-privileged user example)



The command buttons available depend on the privileges of the user and administrator configuration; the following default examples are typical:

- **High-privileged user** - Includes Connect, New, Settings, and Sign-off.
- **Low-privileged user** - Includes Connect, Settings, and Sign-off.
- **Guest user** - Includes Connect, New, Settings, and Sign-off.
- **Stand-alone user** - Includes Connect, New, Settings, and Delete.

Note

If set by the administrator (`enablelocal=yes` in the user.ini/wnos.ini file), High-privileged, Guest, and Low-privileged users will have the Delete command button available instead of the Sign-off command button).

The use associated with these command buttons also depends on user privilege. For example, **Settings** allows a High-privileged user to view and edit connection definitions, while it allows a Low-privileged user to only view connection definitions.

Note

Guest user privileges are determined by the administrator.

The Connect Manager command buttons include:

- **Connect** - To make a connection, select a connection from the list and click **Connect**.
- **New** - Clicking **New** opens the Connection Settings dialog box either directly or through the Connection Protocol menu selection for creating a new connection definition (for more information on the Connection Settings dialog box, refer to "About Configuring ICA and RDP Connections"). The new locally-defined connections are added to the connection list. Be aware of the following information:
  - **High-privileged and Guest user** - Typically, all locally-defined connection definitions are temporary and are lost when the user logs off and when the thin client restarts or is shut down. However, if configured by the administrator

(`enablelocal=yes`), locally-defined connection definitions can be saved in these cases.

- **Stand-alone user** - Locally-defined connections are retained when the thin client restarts or is shut down (there is no individual log-on). Network configuration settings must be made locally.

- **Settings** - Clicking **Settings** opens the Connection Settings dialog box for the selected connection (for more information on the Connection Settings dialog box, refer to "About Configuring ICA and RDP Connections"). Be aware of the following information:
  - **High-privileged user** - Can view and edit the definitions for the currently-selected connection. Edits are not permanently retained when the user signs-off.
  - **Stand-alone user** - Can permanently modify the persistent connections (except when PNAgent/PNLite services are used).
  - **Guest user** - Can modify connections, however, the changes are lost at log-off or restart.
  - **Low-privileged user** - Cannot create or edit connections, but can view connection definitions.
- **Sign-off** - To sign-off from the thin client, click **Sign-off**.
- **Delete** - To delete a connection, select a connection from the list and click **Delete**.

About Configuring ICA and RDP Connections

To open the Connection Settings dialog box for a connection, select the connection you want from the list of available connections in the Connect Manger and click **Settings** (to add new connections, click **New** in the Connect Manager).

For information on configuring ICA connections, refer to "Configuring ICA Connections."

For information on configuring RDP connections, refer to "Configuring RDP Connections."

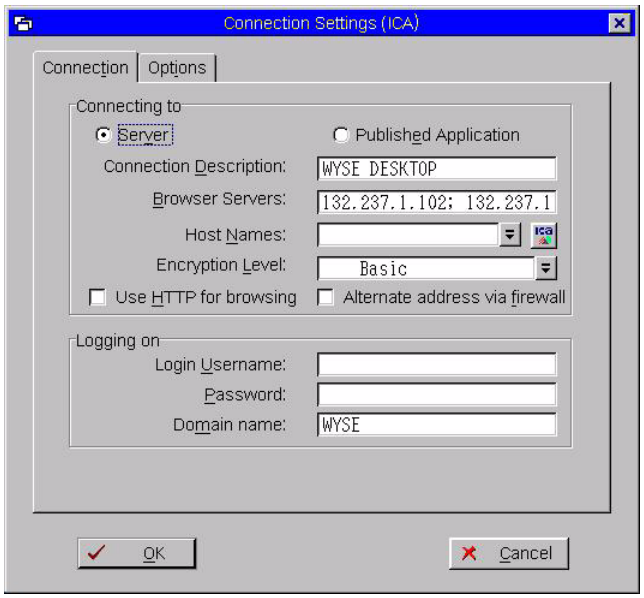
Use the following information when configuring connections (this information assumes that the thin client does not have a locked down privilege level):

- **High-Privileged User** - The additional functionality provided by the Connection Settings dialog box allows testing of connection definitions before they are entered (by the network administrator) into the user profile files.
- **Low-Privileged User** - The settings for the selected connection can be viewed but cannot be edited, and new connections cannot be defined. Connection definitions are controlled by the network administrator and are accessed by the thin client from the user profiles located on a remote server.
- **Guest** - Only connections defined in the Global profile can be viewed.
- **Stand-alone User** - The Connect Manager is available to Stand-alone users because connection definitions cannot be accessed from remote user profiles. If user profiles are available on an FTP server but are not accessed because DHCP is not available or is not configured to provide the file server IP address, the file server IP location can be entered manually using the Network Setup dialog box.

Configuring ICA Connections

If you open the Connection Settings dialog box for an ICA connection (select the ICA connection in the Connect Manger and click **Settings**), you can view and configure the connection (to add new ICA connections, use **New** in the Connect Manager).

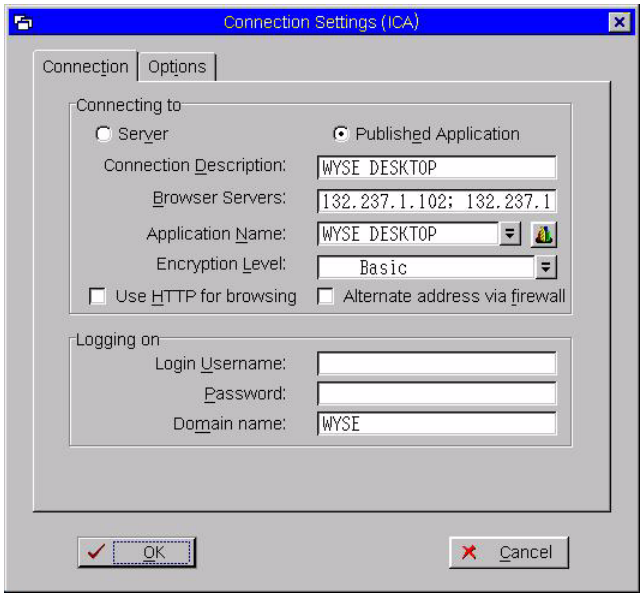
Figure 5 Connection Settings (ICA) - Server option



Note

If you select the Published Application option, the Application Name list box replaces the Host Names list box.

Figure 6 Connection Settings (ICA) - Published Application option



Use the following guidelines:

- **Server** or **Published Application** - Select the type of connection to which the settings apply.
- **Connection Description** - Enter the descriptive name that is to appear in the connection list (38 characters maximum).
- **Browser Servers IP** - Enter a delimited (comma or semicolon) list of IP addresses or DNS-registered names of ICA servers that contains the master browsers list, or that could refer to another server that contains the list. The master browsers list is generated automatically by a browsing program on one of the ICA servers (selected by negotiation between servers). It is used to provide the information displayed in the Server Name or IP list box. No entry is needed if the list is on an ICA server in the same network segment as the thin client. No entry is necessary if the connection is to a server, or if the server name or IP contains the IP address of the server.
- **Host Name** or **Application Name** (title depends on the **Server** or **Published Application** option selected) - You can enter a delimited (semicolon or comma separated) list of server hostnames or IP addresses, or you can select from the list of ICA servers or published applications (depending on **Server** or **Published Application** option selected) obtained from the ICA master browser (you can also use the browse button next to the list box to make the selection you want). If you enter a delimited list of servers, the thin client attempts to connect to the next server on the list if the previous server attempt failed. If you use the list and the selected connection fails, the thin client attempts to connect to the next one on the list.

Note

The Host Name may be resolved using one of three mechanisms: ICA master browser, DNS, or WINS. Master browser is the only mechanism that can resolve a published application (unless manual entry is made in DNS for the application). DNS uses the default domain name in the network control panel to attempt to construct an FQDN but will also try to resolve the name without using the default.

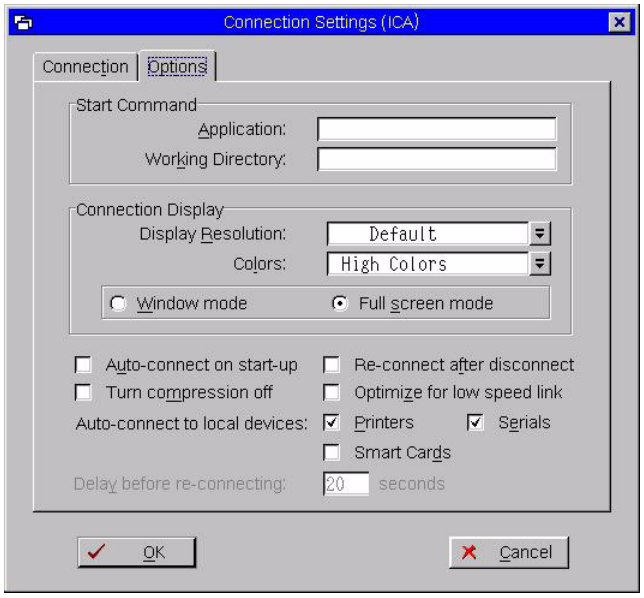
- **Encryption Level** - Allows you to select the security level of communications between the thin client and the ICA server. **Basic** (the default option) is the lowest level of security. Basic allows faster communication between the device and the ICA server because it requires less processing than do the higher levels of encryption.

Caution

The encryption selection applies to the security of communications between the thin client and the ICA server only. It is independent of the security settings of individual applications on the ICA server. For example, most Web financial transactions require the thin client to use 128-bit encryption. However, transaction information could be exposed to a lower level of security if the thin client encryption is not also set to 128 bits.

- **Use HTTP for browsing** - When selected, the thin client by default will use http when browsing.
- **Alternate address via firewall** - When selected, the thin client will use an alternate IP address returned from the ICA master browser to get through firewalls. Used for the Windows log-on when the connection is activated.
- **Logging on** area - Enter login username, password, and domain name. If these boxes are not populated, you can enter the information manually in the ICA server login screen when the connection is made. Use the following guidelines:
  - **Login Username** - 31 characters maximum.
  - **Password** - 19 characters maximum.
  - **Domain Name** - 31 characters maximum.

Figure 7 Connection Settings (ICA) - Options tab



Use the following guidelines:

- **Application** (127 characters maximum) and **Working Directory** (63 characters maximum) - Enter an initialization string and arguments, including an associated working directory, that you want to start automatically on the server when the connection is made.

Note

This area is disabled (grayed) for a published application option.

- **Display Resolution** - Select the display resolution for this connection. Selections include (If you select the **Published Application** option, the Connection Display will allow you to select the **Seamless Display Resolution** option):
  - **Default**
  - **640 x 480**
  - **800 x 600**
  - **1024 x 768**
  - **1280 x 1024**
  - **1600 x 1200**
- **Colors** - Select the color depth of the ICA session. If **High Colors** (16 bits) or **True Colors** is selected and the ICA server does not support this color depth, the thin client renegotiates the color depth to the lower value (for example, **256 Colors** (8bits)).

Note

If you select the **Published Application** option, the Connection Display will allow you to select the **True Colors** (1600 x 1200) option.

- **Window mode** and **Full screen mode** - Select the initial view of the application in a windowed screen or full screen. You can toggle between viewing modes by using CTRL+ALT+UPARROW.
- **Auto-connect on start-up** - When selected, automatically connects the session on start-up.

- **Re-connect after disconnect** - When selected, causes the thin client to automatically reconnect to a session after a non-operator-initiated disconnect. If selected, the wait interval is that set in the **Delay before re-connecting** box or the user profile for *yes* (20 seconds) or *seconds*. The default is 20 seconds if there is no ini file description of this connection, or is a Stand-alone user, or simply omitted.
- **Turn compression off** - When selected, turns compression off (intended for high-speed connections).
- **Optimize for low speed link** - When selected, allows optimization for low-speed connections, such as reducing audio quality and/or decreasing protocol-specific cache size. Intended for a connection spanning a WAN link or using dialup.
- **Auto-connect to local devices** - Select any of the options (**Printers**, **Serials**, and **Smart Cards**) to have the thin client automatically connect to the devices (an ICA session will not automatically connect to a device through a serial port).
- **Delay before re-connecting** - Becomes active if **Re-connect after disconnect** is selected. Enter the number of seconds (1 to 3600) before trying to reconnect after a disconnect.

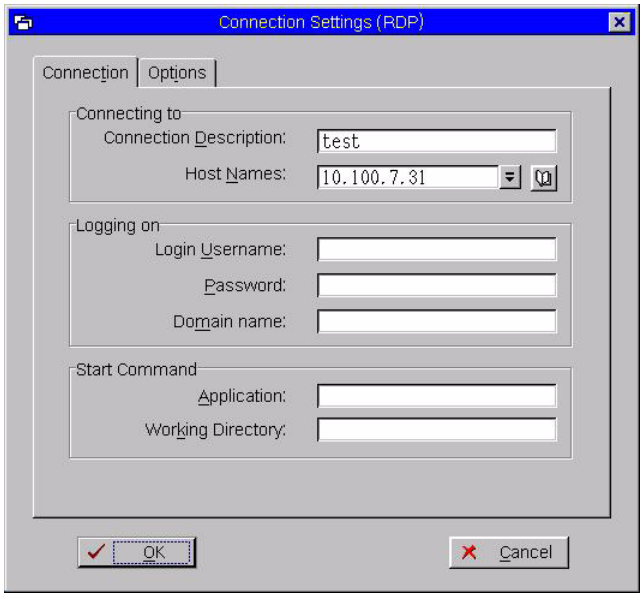
Configuring RDP Connections

If you open the Connection Settings dialog box for an RDP connection (select the RDP connection in the Connect Manger and click **Settings**), you can view and configure the connection (to add new RDP connections, use **New** in the Connect Manager).

Note

In a Virtual Desktop environment, an RDP connection will be assigned by the Virtual Desktop Broker; you do not need to create an RDP connection manually.

Figure 8 Connection Settings (RDP) - Connection tab



Use the following guidelines:

- **Connection Description** - Enter the descriptive name that is to appear in the connection list (38 characters maximum).
- **Host Names** - Use the list to select the valid DNS server name or the IP address of the server to which the thin client connection is to be made (you can also use the browse

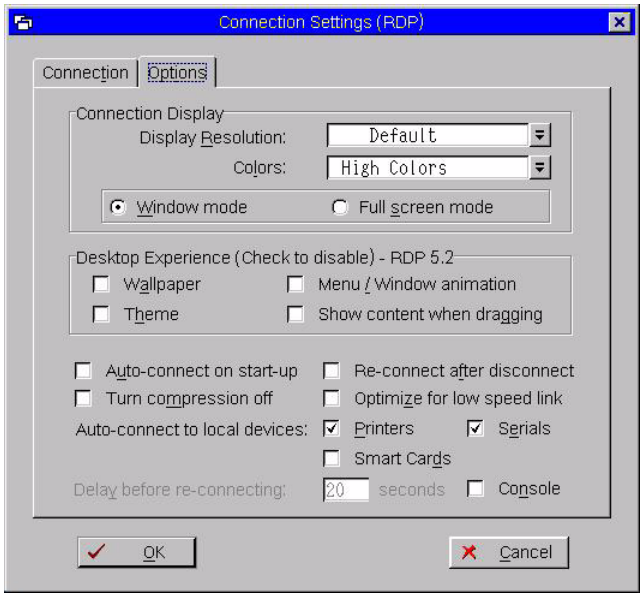
button next to the list box to make the selection you want). For example, a list of WTS servers on the local network from which you can select.

Note

The server name may be resolved using one of two mechanisms: DNS, and WINS. DNS uses the default domain name in the network control panel to attempt to construct an FQDN but will also try to resolve the name without using the default.

- **Logging on** area - Enter login username, password, and domain name. If these boxes are not populated, you can enter the information manually in the RDP server login screen when the connection is made. Use the following guidelines:
  - **Login Username** - 31 characters maximum.
  - **Password** - 19 characters maximum.
  - **Domain Name** - 31 characters maximum.
- **Application** (127 characters maximum) and **Working Directory** (63 characters maximum) - Enter an initialization string and arguments, including an associated working directory, that you want to start automatically on the server when the connection is made.

Figure 9 Connection Settings (RDP) - Options tab



Use the following guidelines:

- **Display Resolution** - Select the display resolution for this connection. Selections include:
  - **Default**
  - **640 x 480**
  - **800 x 600**
  - **1024 x 768**
  - **1280 x 1024**
  - **1600 x 1200**

- **Colors** - Select the color depth of the RDP session. If **High Colors** (16 bits) or **True Colors** is selected and the RDP server does not support this color depth, the thin client renegotiates the color depth to the lower value (for example, **256 Colors** (8bits)).

Note

For some thin clients versions, only the 256 Colors (8 bits) selection is available for RDP connections. Also, for older versions of the server software (for example, RDP 4.0) the server only supports 8 bit color. This is not detectable in advance but results in use of 8 bit color when the connection is established.

- **Window mode** and **Full screen mode** - Select the initial view of the application in a windowed screen or full screen. You can toggle between viewing modes by using CTRL+ALT+UPARROW.
- **Wallpaper** - When selected, disables the desktop wallpaper.
- **Menu / Window animation** - When selected, disables the menu or window animation character.
- **Theme** - When selected, disables the desktop themes.
- **Show content when dragging** - By default, when you grab a Window by the title bar and move it around, the contents of the window will move with it. Select this to disable this content view so that only the outline of the window moves when dragging it, until you drop the window. This option can be beneficial, as it uses less processing power.
- **Auto-connect on start-up** - When selected, automatically connects the session on start-up.
- **Re-connect after disconnect** - When selected, causes the thin client to automatically reconnect to a session after a non-operator-initiated disconnect. If selected, the wait interval is that set in the **Delay before re-connecting** box or the user profile for *yes* (20 seconds) or *seconds*. The default is 20 seconds if there is no ini file description of this connection, or is a Stand-alone user, or is simply omitted.
- **Turn compression off** - When selected, turns compression off (intended for high-speed connections).
- **Optimize for low speed link** - When selected, allows optimization for low-speed connections, such as reducing audio quality and/or decreasing protocol-specific cache size. Intended for a connection spanning a WAN link or using dialup.
- **Auto-connect to local devices** - Select any of the options (**Printers**, **Serials**, **Smart Cards**) to have the thin client automatically connect to the devices.
- **Delay before re-connecting** - Becomes active if **Re-connect after disconnect** is selected. Enter the number of seconds (1 to 3600) before trying to reconnect after a disconnect.
- **Console** - Select to set the RDP connection with Console mode.

This page intentionally blank.

3 Setting Up the Thin Client

This chapter contains information to help you set up your thin client using the System Setup submenu.

Since the setup information for individual users (user profile) is stored in a remote database, very little setup is required of a thin client operator. Your user profile is loaded into the thin client when you log-on. For this reason, you can log-on to another thin client (under the same account name) and see the same user profile settings.

A few setup items are reserved for local selection (not available to Non-privileged users). They are available locally because they are user preference items or pertain to the thin client hardware rather than the person using the thin client. Additional local settings may be required if some of the network services are not available. Generally, the defaults and initial setup configurations are adequate and any changes should be made under guidance of the network administrator.

To access the local setup menus (System Settings submenu), click the User Name button (located at the bottom-left side of the taskbar), and select **System Setup**.

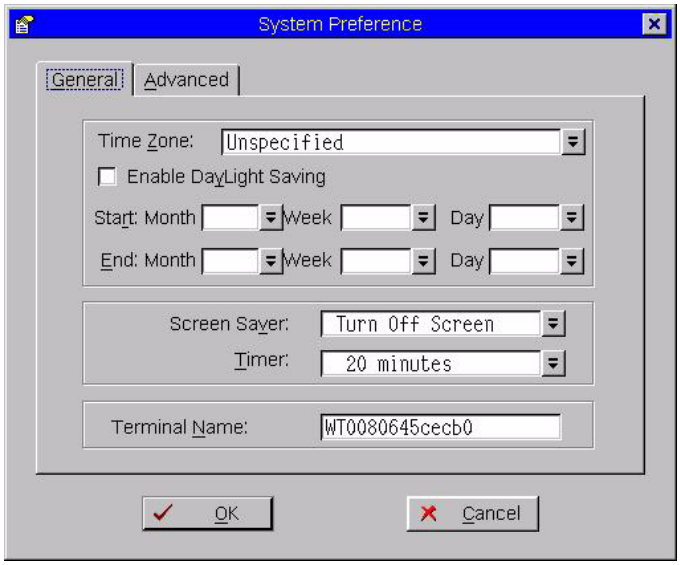
The System Setup submenu provides access to local system setup dialog boxes for:

- “Setting System Preferences”
- “Configuring Network Settings”
- “Setting Up Wireless Access”
- “Selecting Display Settings”
- “Configuring Serial Communications”
- “Setting Up Printers”
- “Configuring Touch Screens”

Setting System Preferences

The System Preference dialog box allows you to select personal preferences such as time zone, screen saver, mouse speed and left/right buttons, keyboard language, and so on.

Figure 10 System Preference - General tab



Use the following guidelines:

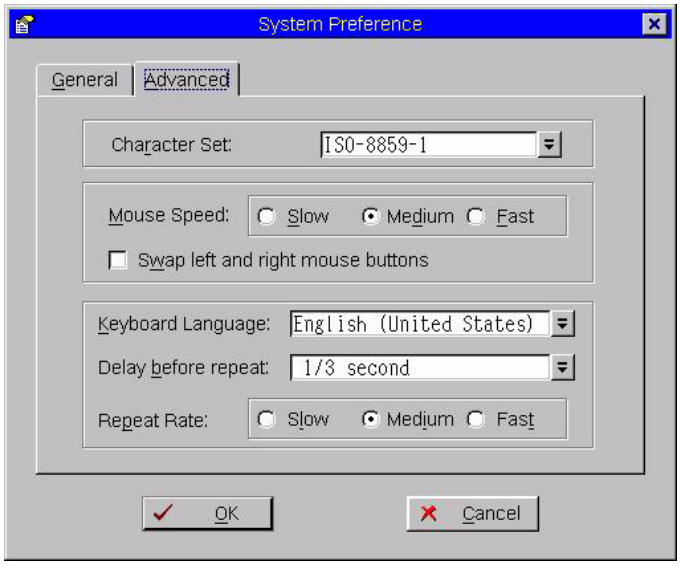
- **Time Zone** - Allows you to select a time zone where the terminal operates (default is **Unspecified**).

Note

Time zone is supported by MetaFrame XP FR2 release or later.

- **Enable Daylight Saving** - Allows you to enable the daylight saving settings. When selected, the six list boxes must be properly configured to define the daylight saving starting (month/week/day) and ending (month/week/day) periods. Use the following guidelines:
  - **Month** - Specifies the month in the year from **January** through **December**.
  - **Week** - Select **1** through **4** for the week in the month. Week **Last** denotes the last week in the month.
  - **Day** - Specifies the day of the week from **Monday** through **Sunday**.
- **Screen Saver** - Allows you to select the type of screen saver you want. The default is to **Turn Off Screen**. Other selections available include **Flying Bubbles** and **Moving Image** (which are screen savers with the monitor remaining on).
- **Timer** - Select a time after which the screen saver is to be activated (default is 20 minutes). When the thin client is left idle for the specified idle time, the screen saver is initiated.
- **Terminal Name** - Allows entry of a name for the thin client. The default is a 14-character string composed of the letters WT followed by the thin client Ethernet MAC address. Some DHCP servers use this value to identify the IP address lease in the DHCP Manager display.

Figure 11 System Preference - Advanced tab



- **Character Set** - Select the character set (Each character is represented by a number. The ASCII character set, for example, uses the numbers 0 through 127 to represent all English characters as well as special control characters. European ISO character sets are similar to ASCII, but they contain additional characters for European languages).
- **Mouse Speed** and **Swap left and right mouse buttons** - Select the mouse speed. You can also swap mouse buttons for left-handed operation by selecting **Swap left and right mouse buttons**. If the mouse is changed for use by a left-handed person, the mouse arrow points right for a local session only. It reverts back to a left-pointing arrow when an ICA or RDP session opens.
- **Keyboard Language** - Currently the following keyboard languages are supported (default i**s English (United States)**).

Table 1 Supported Keyboard Languages

Supported Keyboard Languages		
Arabic (Saudi Arabia)	Chinese (Traditional)	Hungarian
Arabic (Iraq)	Croatian	Italian
Arabic (Egypt)	Czech	Italian (Swiss)
Arabic (Libya)	Danish	Japanese
Arabic (Algeria)	Dutch	Korean
Arabic (Morocco)	Dutch (Belgian)	Norwegian
Arabic (Tunisia)	English (Australian)	Polish (214)
Arabic (Oman)	English (3270 Australian)	Polish Programmers
Arabic (Yemen)	English (New Zealand)	Portuguese
Arabic (Syria)	English (United Kingdom)	Romanian
Arabic (Jordan)	**English (United States)**	Slovakian
Arabic (Lebanon)	Finnish	Slovakian (Qwerty)
Arabic (Kuwait)	French (Belgian)	Slovenian
Arabic (U.A.E.)	French (Canadian)	Spanish
Arabic (Bahrain)	French (France)	Spanish (Mexican)
Arabic (Qatar)	French (Swiss)	Swedish
Brazilian	German	Turkish
Canadian (Multilingual)	German (Swiss)	Turkish (QWERTY)
Chinese (Simplified)	Greek	U.S. International

- **Delay before repeat** - Repeat parameters for held-down key. Delay before repeat selectable from **1/5 second** to **2 seconds**, or **no repeat**. The default is **1/3 second**.
- **Repeat Rate** - Select **Slow**, **Medium**, or **Fast**. The default is **Medium**.

Configuring Network Settings

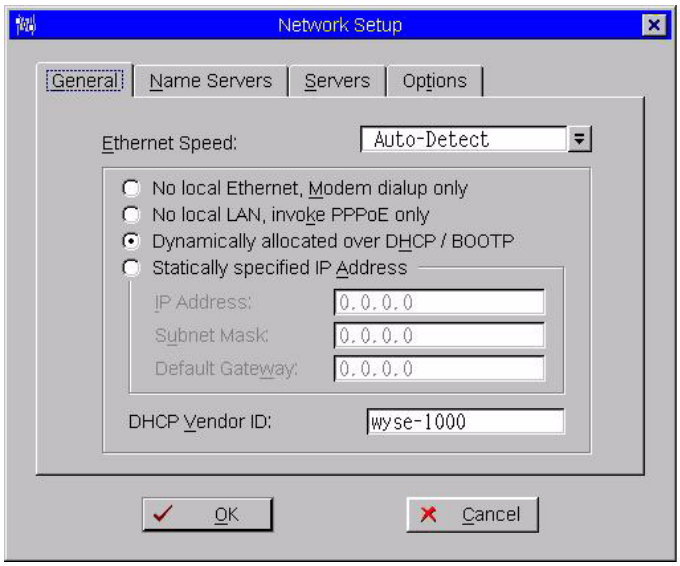
The Network Setup dialog box allows you to configure thin client network settings (including operation in modem dialup and PPPoE modes, as well as locations of servers essential to thin client operation).

Note

If required by the operating environment, the network administrator may disable access to this dialog box. Specifically, it cannot be accessed by Non-privileged and Low-privileged users (and not until after log on if using dial-up or PPPoE access). In addition, if the network administrator has set the lockdown mode by means of an entry in the user profile, both system reset and access to this dialog box are disabled for Stand-alone users as well.

For more information about system lockdown, refer to "Understanding System Lock-down."

Figure 12 Network Setup - General tab



Use the following guidelines:

- **Ethernet Speed** - Normally the default (**Auto-Detect**) should be selected, but another selection can be made if automatic negotiation is not supported by your network equipment. Selections include **Auto-Detect**, **10 Mb Half-Duplex**, **10 Mb Full-Duplex**, **100 Mb Half-Duplex**, **100 Mb Full-Duplex**.

Note

The **10 Mb Full-Duplex** option can be selected locally at the device, however, this mode may need to be negotiated through **Auto-Detect**.

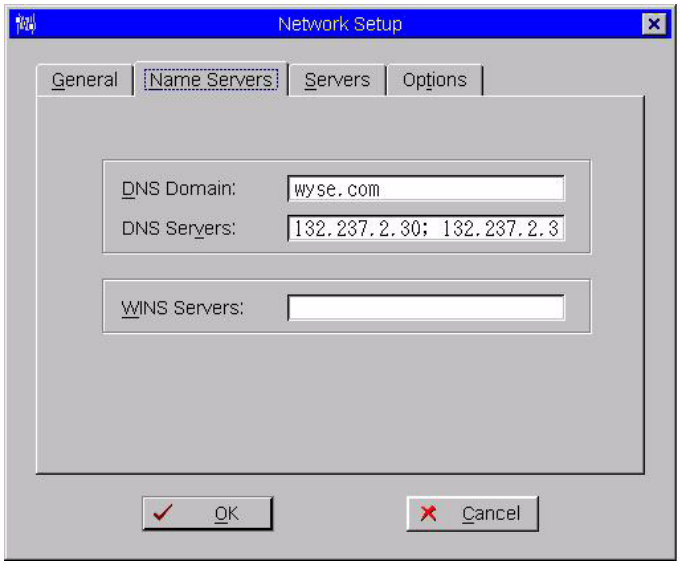
- **No local Ethernet, Modem dialup only** - Select this option if the thin client will access a network through a dial-up modem (for more information, refer to "Configuring Dialup Modem Access"and "Configuring Serial Communications."
- **No local LAN, invoke PPPoE only** - Select this option if the thin client will access a network through a PPPoE connection. For more information, refer to "Configuring PPPoE Access."
- **Dynamically allocated over DHCP/BOOTP** - Selecting this option enables the thin client to automatically receive (from the DHCP server) the following:
  - All network settings, including its IP address and the location of the file server.
  - A list of PNAgent/PNLite servers that may be used to obtain a list of published applications.
  - A list of Windows domains that can be selected for use when authenticating a user for PNAgent/PNLite.
  - An FTP user name and password to be authenticated when using non-anonymous FTP server access.
  - A list of Rapport servers and the TCP port to be used when contacting those servers.

Note

The network administrator must configure the DHCP server to provide this information. Any value provided by the DHCP server will replace any information entered locally however, that locally entered information will be used if the DHCP server fails to provide replacement values.
If the thin client is to be used as an LPD server, DHCP cannot be used and a static IP address must be assigned (see “Configuring LPD Services”).

- **Statically specified IP Address** - Select this option to manual enter the IP Address, Subnet Mask, and Default Gateway.
  - **IP Address** - Must be a valid network address in the thin client server environment. The network administrator must provide this information.
  - **Subnet Mask** - Enter the value of the subnet mask. A subnet mask is used to gain access to machines on other subnets. The subnet mask is used to differentiate the location of other IP addresses with two choices: same subnet or other subnet. If the location is other subnet, messages sent to that address must be sent through the Default Gateway, whether specified through local configuration or through DHCP. Ask the network administrator for this value.
  - **Default Gateway** - Use of gateways is optional. Gateways are used to interconnect multiple networks (routing or delivering IP packets between them). The default gateway is used for accessing the Internet or an intranet with multiple subnets. If no gateway is specified, the thin client can only address other systems on the same subnet. Enter the address of the router that connects the thin client to the Internet. The address must exist on the same subnet as the thin client as defined by the IP address and the subnet mask. If DHCP is used, the address can be supplied through DHCP.
- **DHCP Vendor ID** - Shows the DHCP Vendor ID when the **Dynamically allocated over DHCP / BOOTP** option is selected.

Figure 13 Network Setup - Name Servers tab



Use the following guidelines:

- **DNS Domain** and **DNS Servers** - Use of DNS is optional. DNS allows you to specify remote systems by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it rather than DNS will be used to make the connection. Enter the DNS Domain and the network address of an available DNS Server. The function of the DNS Domain entry is to provide a default suffix to be used in name resolution. The values for these two boxes may be supplied by a DHCP server. If the DHCP server supplies these values, they will replace any locally configured values. If the DHCP server does not supply these values, the locally configured values will be used.

Note

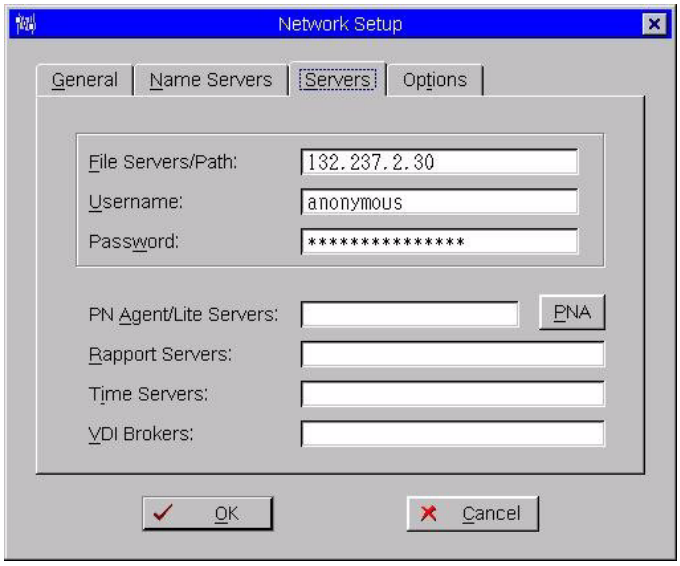
You may enter two DNS Server addresses, separated by a semicolon, comma, or space. The first address is for the primary DNS server and the second is for a backup DNS server.

- **WINS Servers** - Use of WINS is optional. Enter the network address of an available WINS name server. WINS allows you to specify remote systems by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it rather than WINS will be used to make the connection. These entries can be supplied through DHCP if DHCP is used. DNS and WINS provide essentially the same function, name resolution. If both DNS and WINS are available, the thin client will attempt to resolve the name using DNS first and then WINS.

Note

You may enter two WINS Server addresses, separated by a semicolon, comma, or space. The first address is for the primary WINS server and the second is for a backup WINS server.

Figure 14 Network Setup - Servers tab



Use the following guidelines:

- **File Servers/Path**, **Username**, and **Password** - IP address or host name of the FTP server that provides the system software and update images. The address can be supplied through DHCP if DHCP is used. Use the following guidelines:
  - **File Servers/Path** - Allows 128 characters maximum. The data specifies part of the path to be used when the server is accessed. Multiple file servers/paths may be named, as long as all data fits in the length limitation.
  - **Username** - To log in to the FTP server. Use 15 characters maximum.
  - **Password** - To log in to the FTP server. Use 15 characters maximum.

Note

The FTP server also provides Global and User profiles (if they exist), optional custom bitmaps to modify the appearance of the login window (if used), and bitmaps for custom icons to be used when displaying connections on the desktop.

- **PN Agent/Lite Servers**, **Rapport Servers**, **Time Servers** and **VDI Brokers** - List of IP addresses or host names with optional TCP port number of Time servers. Each entry with optional port number is specified as Name-or-IP:port, where :port is optional. If not specified, port 80 is used. Locations can be supplied through user profiles if user profiles are used. The Time server(s) provide thin client time based on the settings of time zone and daylight saving information. If DHCP is used, locations can be supplied through DHCP. You can also click the **PNA** command button to open the Reconnect Options dialog box, and further configure the connection for automatic reconnection.

Note

The Virtual Desktop Broker supports both http and https, and depends on the Virtual Desktop Broker server support. If http or https is not specified on the Virtual Desktop Broker server, then http is used by default. If https is specified, the client side must install a corresponding root certificate.
After making a **VDI Brokers** entry, be sure to reboot the thin client to have the changes take effect.

Figure 15 Network Setup - Reconnect options

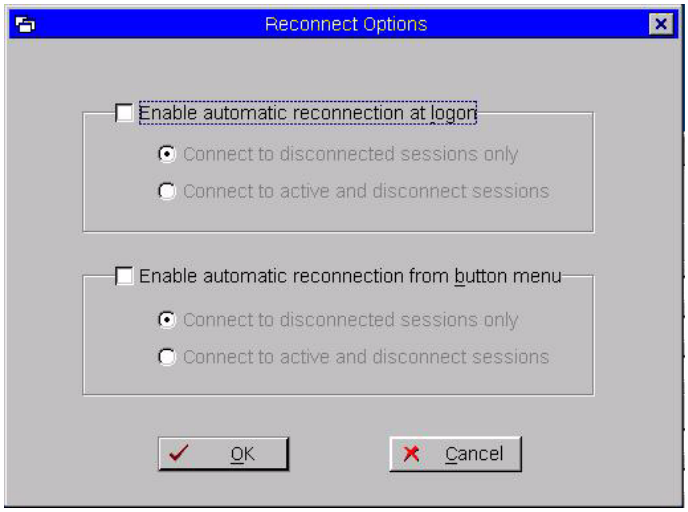
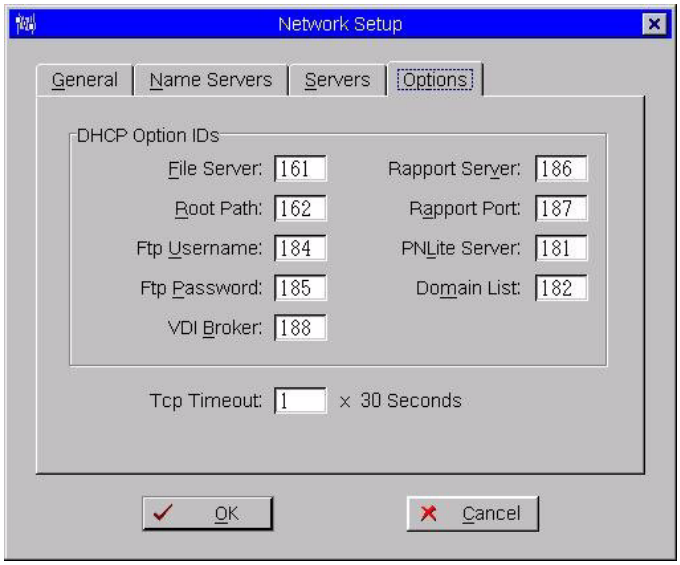


Figure 16 Network Setup - Options tab



Use the following guidelines:

- **DHCP Option IDs** - Enter the supported DHCP options (each value can only be used once and must be between **128** and **254**). For information on DHCP options, refer to the *Administrators Guide: Wyse® Winterm™ 1 series, Based on Wyse Thin OS*.
- **Tcp Timeout** - Enter the number of 30 seconds for the timeout value of a TCP connection. The value must be between **1** and **255** which means the connection timeout value is from 1x30 seconds to 255x30 seconds.

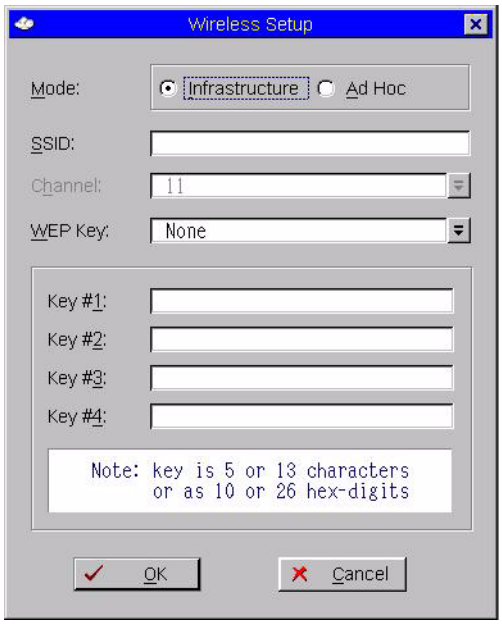
Setting Up Wireless Access

The Wireless Setup dialog box allows you to configure the parameters required for wireless wide-band modem access to the enterprise intranet.

A wireless wide-band network device can be used to access the enterprise intranet. The wireless network device connects to a USB port on the thin client and uses short-range wide-band radio to communicate with a wireless access point. Typically, wireless access points are located at several locations in the enterprise within range of the wide-band modems, and connect directly to the enterprise intranet.

Service Set Identification (SSID), Channel, and encryption keys (WEP keys) must be entered in the Wireless Setup dialog box on the thin client. Corresponding entries must also be made in the enterprise access point (except for this, thin client operation is the same as Ethernet direct access, including access to the enterprise DHCP server).

Figure 17 Wireless Setup



Use the following guidelines:

- Network **Mode** options:
  - **Infrastructure** (default) - This mode of operation requires the presence of an IEEE specification 802.11b-compliant access point. All communication is done through the access point which relays packets to other wireless clients as well as to nodes on a wired Ethernet network.
  - **Ad Hoc** - This is the IEEE 802.11b peer-to-peer mode of operation. In this mode, only one wireless cell is supported for each different Service Set Identification (SSID). All communication is done client-to-client without the use of an access point.
- **SSID** - Enter the Service Set Identification set up by the network administrator for this wireless communication link.
- **Channel** - Select the frequency channel (**0** through **14**) to be used for this wireless communication link (the channel can only be selected in Ad Hoc mode, as the channel is selected based on the relative strength of signals from the available access points in Infrastructure mode).
- **WEP Key** - Wired Equivalent Privacy (WEP) encryption can be enabled by selecting one of the keys in the list corresponding to those entered in the **Key #1** through **Key #4** boxes. Select **None** if encryption is not required. WEP uses the selected key to

encrypt/decrypt each frame transmitted from or received by the wireless adapter. The access point must recognize frames encrypted by the same key.

- **Key #1** through **Key #4** boxes - Enter the encryption keys provided by the network administrator. The **WEP Key** selection determines which key is used for encryption.

Selecting Display Settings

The Display Setup dialog box allows you to select the resolution and refresh rate for the monitor used with the thin client. The number of icons that can be displayed on the desktop depends on the desktop resolution and administrator configuration.

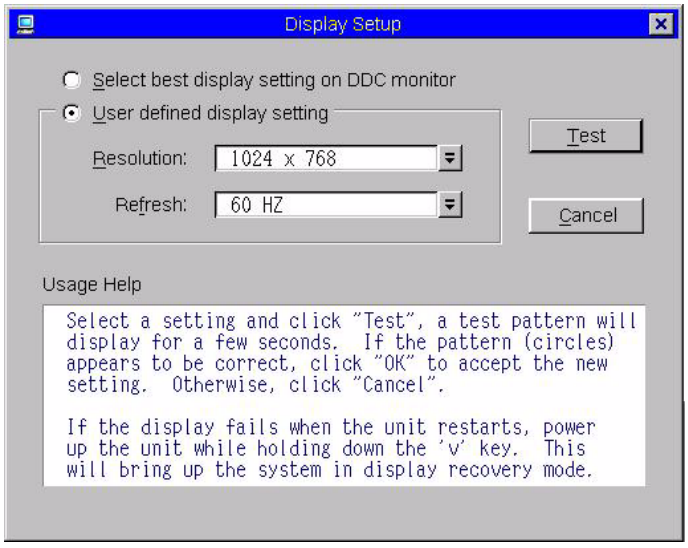
Note

On thin clients that only support 8 bit color, the 1280 x 1024 resolution will be used to display full screen connections. The 1280 x 1024 resolution will not be used to display the desktop, windowed connections, or seamless connections.

If configured by your administrator (`Longapplicationname=yes` as defined in wnos.ini), the number of icons displayed for a resolution is as follows:

- 640 x 480: Up to 8 icons are displayed.
- 800 x 600: Up to 10 icons are displayed.
- 1024 x 768: Up to 21 icons are displayed.
- 1280 x 1024: Up to 40 icons are displayed.
- 1600 x 1200: Up to 60 icons are displayed.

Figure 18 Display Setup



Use the following guidelines:

- **Select best display setting on DDC monitor** - If the monitor is VESA DDC2B (Display Data Channel) compatible, selection of this option allows the thin client to automatically select the best resolution and refresh rate. If your monitor is not DDC compatible, a *Monitor does not support Plug and Play* message is displayed (click **OK** to acknowledge the message and remove it from the screen).

- **User defined display setting** - Select this option and select the resolution and refresh rate supported by your monitor (all combinations are allowed):
  - **Resolution** list selections include:
    640 x 480
    800 x 600 (default)
    1024 x 768
    1280 x 1024
    1600 x 1200
  - **Refresh** rate list selections include:
    60 Hz (default)
    75 Hz
    85 Hz
- **Usage Help** area - Contains brief instructions for using the Display Setup dialog box and running the test. No operator entry can be made in this box. Make note of the instructions in the area regarding v-key reset usage in case of display failure.

Configuring Serial Communications

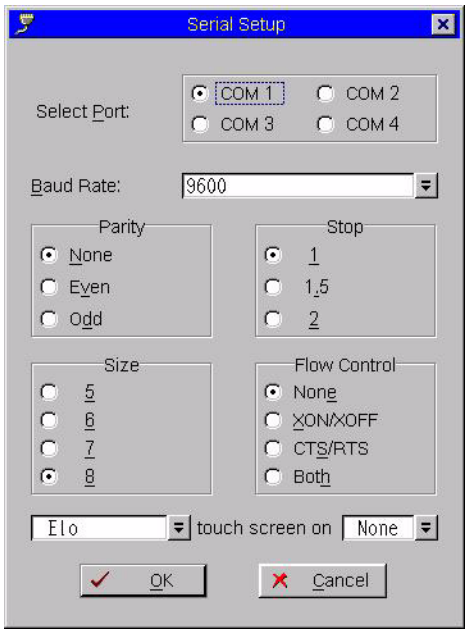
The Serial Setup dialog box allows configuration of the ports used for modem dialup mode and serial communications.

A serial port can be used for modem access to a network (intranet or Internet) through a dial-up server (for example, a Microsoft Remote Access Server, or an ISP supporting industry-standard protocols) as an alternative or supplement to using the thin client network port (see “Using and Configuring Access Connections”). For this use, a USB modem or a converter and a serial modem must be connected to the thin client USB port. A USB hub may be employed to support up to two USB ports if another USB connector is not available on your thin client (see "Configuring Dialup Modem Access"). For supported converters, refer to the Wyse Web site.

Note

With Wyse software version 4.2 and later, ICA virtual COM driver supports synchronizing with Palm devices over a serial port.

Figure 19 Serial Setup



Use the following guidelines:

- **Select Port** - Select the port to which this setup definition applies. Either Port **1**, **2**, **3**, or **4** can be selected (default is Port **1**). For Model SX0, Product S10, **COM 1** or **COM 2** selects from either the USB or serial device.
- **Baud Rate** - Either **1200**, **2400**, **4800**, **9600**, **19200**, **38400**, **57600**, or **115200** baud can be selected (default is **9600**).
- **Parity** - Either **None**, **Even**, or **Odd** can be selected (default is **None**).
- **Stop** - Either **1**, **1.5**, or **2** stop bits can be selected (default is **1**).
- **Size** - Character size **5**, **6**, **7**, or **8** bits can be selected (default is **8**).
- **Flow Control** - Either **None**, **XON/XOFF**, **CTS/RTS**, or **Both** can be selected (default is **None**).
- Serial Touch Screen selections - Select the proper touch screen **ELO**, **MicroTouch** or **FastPoint** from the list.
- **Touch Screen on** - Select the proper serial port (COM port) or **None** from the list.

Setting Up Printers

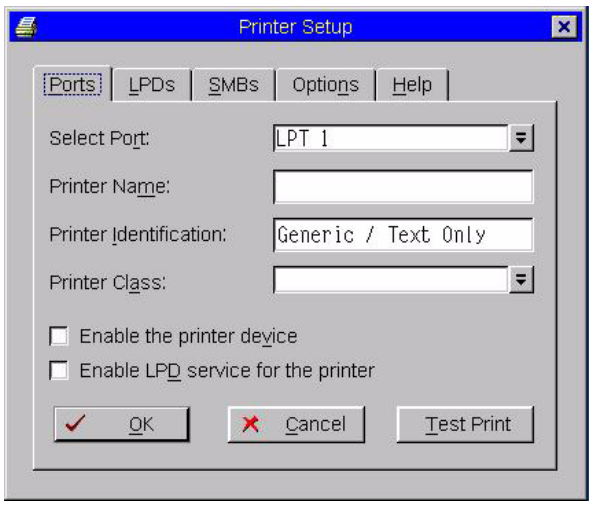
The Printer Setup dialog box allows configuration of network printers and local printers that are connected to the thin client (USB and Serial). Through its USB ports, a thin client can support multiple printers. If more than one printer is to be used and another port is not available on your thin client and the port that is to be used must be shared with a USB modem converter, connect a USB hub to the port.

Note

If required, USB-to-Parallel and USB-to-Serial converter cables are available from Wyse Technology. Port LPT1 or LPT2 selects the connection to a USB printer or parallel printer through a USB-to-Parallel cable. Port COM1 or COM2 selects the connection to a serial device through a USB-to-Serial cable. For ordering information, refer to the Wyse Web site at: http://www.wyse.com/products/accessories/accessories.asp.

Typically, printers are also available through the application sessions. This can include network printers and printers locally connected to the application servers. When connecting to a Citrix server, the locally connected printer shows as the default printer.

Figure 20 Printer Setup - Ports tab



Use the following guidelines:

- **Select Port** - Select the port you want from the list.
- **Printer Name** - This is a required entry. If **Enable LPD service for the printer** is selected, the printer name becomes the queue name for other clients using LPR to print to this printer.
- **Printer Identification** - Enter the type or model of the printer. This name should be either the device driver name for the printer under the Microsoft Windows system, or a key to map to the device driver. If not specified, the name will be defaulted to the printer-supplied identification for standard direct-connected USB printers or **Generic / Text Only** for non-USB or serial-connected printers upon connection to Windows hosts. The driver name mapping takes place either through a printer-mapping file read by the system as part of the Global system profile (wnos.ini) or by MetaFrame servers through the MetaFrame printer configuration file (\winnt\system32\wtsprnt.inf).

Note

Most USB direct-connected printers or parallel printers connected through USB-to-parallel cable converters do report their printer identifications. Port LPT1 or LPT2 selects the connection to a USB printer or parallel printer through a USB-to-Parallel cable. Port COM1 or COM2 selects the connection to a serial device through a USB-to-Serial cable.

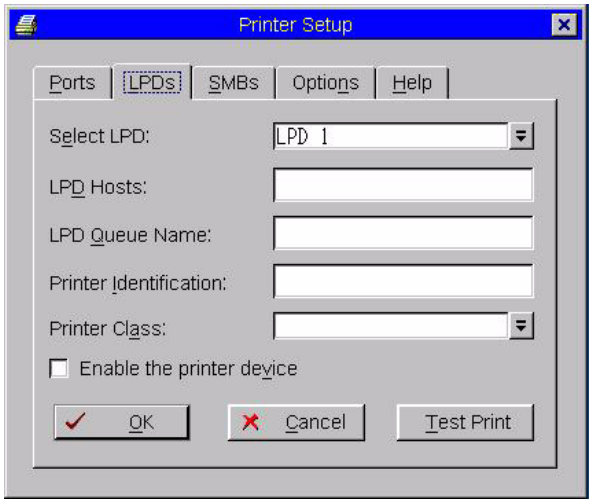
In an ICA environment, it is recommended that administrators use the `wtsprnt.inf` file to define printer driver mapping to maintain the consistency of usage from various ICA client devices. In an RDP environment, administrators should use the `wnos.ini` file to define printer driver mapping. If there is no mapping file, or if the mapping entry for the printer is not found, the identification must be a supported driver name on the connected hosts for the printer to be automatically created on the hosts.

- **Printer Class** - Select the printer class from the list.
- **Enable the printer device** - This must be selected to enable the directly-connected printer.
- **Enable LPD service for the printer** - Select this to make the thin client an LPD (Line Printer Daemon) server for LPD printing requests from the network (see “Configuring LPD Services”).

Note

If the thin client is to be used as an LPD printer server, DHCP must not be used and a static IP address must be assigned to the thin client (see “Configuring Network Settings” for more details).

Figure 21 Printer Setup - LPDs tab



Use the following guidelines:

- **Select LPD** - Select the port you want from the list.
- **LPD Hosts** - The DNS or WINS name of the server for the network printer. An IP address can also be entered.

Note

If the printer is attached to another thin client on your network, the entry in the LPD Hosts box is the name or address of that thin client.

- **LPD Queue Name** - An LPD host maintains a named queue for each supported printer. Enter the name of the queue associated with the printer to be used.

Note

The LPD Queue Name must match the content of the Printer Name box on the thin client with the printer attached.

- **Printer Identification** - Enter the type or model of the printer. This name should be either the device driver name for the printer under the Microsoft Windows system, or a key to map to the device driver. If not specified, the name will be defaulted to the printer-supplied identification for standard direct-connected USB printers or Generic / Text for non-USB or serial-connected printers upon connection to Windows hosts. The driver name mapping takes place either through a printer-mapping file read by the system as part of the Global system profile (wnos.ini) or by MetaFrame servers through the MetaFrame printer configuration file (\winnt\system32\wtsprnt.inf).

Note

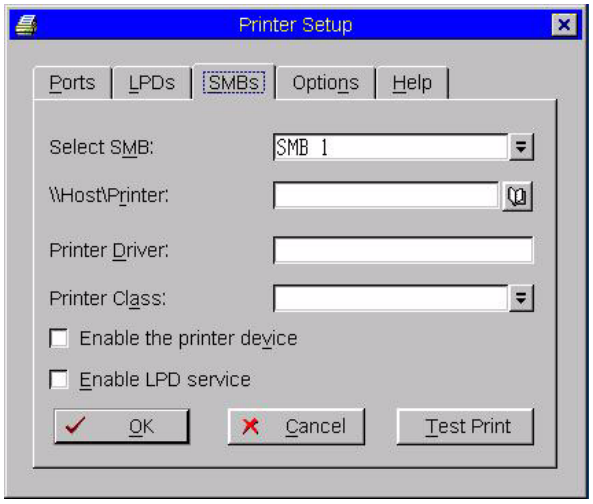
Most USB direct-connected printers or parallel printers connected through USB-to-parallel cable converters do report their printer identifications. Port LPT1 or LPT2 selects the connection to a USB printer or parallel printer through a USB-to-Parallel cable. Port COM1 or COM2 selects the connection to a serial device through a USB-to-Serial cable.

In an ICA environment, it is recommended that administrators use the `wtsprnt.inf` file to define printer driver mapping to maintain the consistency of usage from various ICA client devices. In an RDP environment, administrators should use the `wnos.ini` file to define printer driver mapping. If there is no mapping file, or if the mapping entry

for the printer is not found, the identification must be a supported driver name on the connected hosts for the printer to be automatically created on the hosts.

- **Printer Class** - Select the printer class from the list.
- **Enable the printer device** - This must be selected to enable the directly-connected printer.

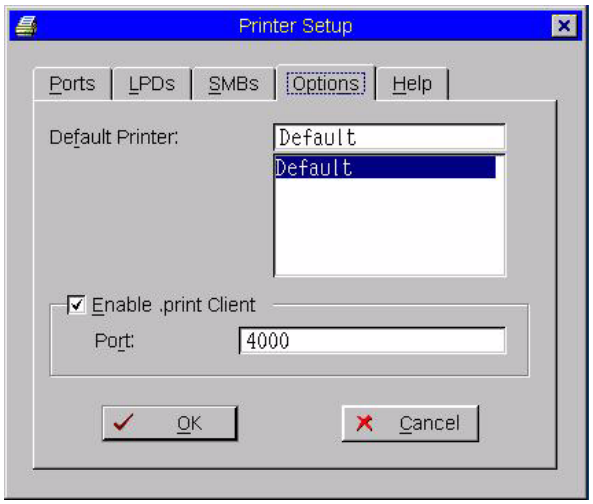
Figure 22 Printer Setup - SMBs tab



Use the following guidelines:

- **Select SMD** - Select the SMB you want from the list.
- **\\Host\Printer** - Enter the Host\Printer or use the browse button next to the box to make the selection you want.
- **Printer Driver** - Enter the printer driver you require.
- **Printer Class** - Select the printer class from the list.
- **Enable the printer device** - This must be selected to enable the directly-connected printer.
- **Enable LPD service** - Select this to make the thin client an LPD (Line Printer Daemon) server for LPD printing requests from the network (for more information refer to "Configuring LPD Services."

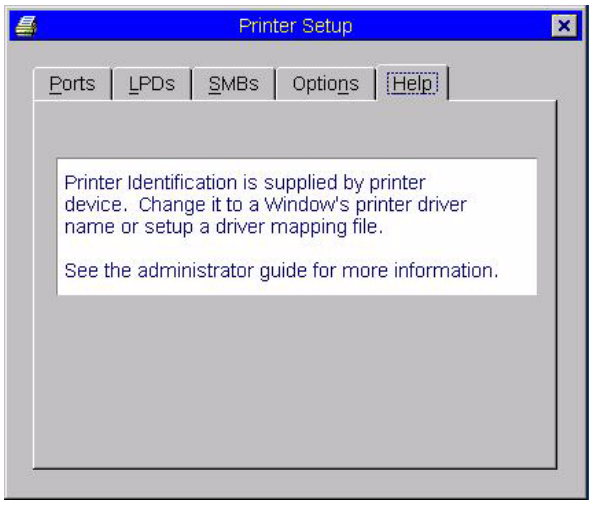
Figure 23 Printer Setup - Options tab



Use the following guidelines:

- **Default Printer** - Select the printer you want to be the default printer from the list.
- **Enable .print Client** and **Port** - If you want to enable .print Client, select **Enable .print Client** and then enter the port.

Figure 24 Printer Setup - Help tab



The Help tab contains printer help information.

Configuring LPD Services

A thin client can be configured to provide LPD (Line Printer Daemon) services, making the thin client a printer server on the network.

Set-up the thin client that is to provide LPD print services as follows:

1. Open the Network Setup dialog box (**Desktop Menu | System Setup | Network**) and enter a static IP address for the thin client (ask your network administrator for an IP address).
2. Open the Printer Setup dialog box (**Desktop Menu | System Setup | Printer**) and select any of the listed ports.
3. Name the printer in the Printer Name box.
4. Select **Enable LPD service for the printer**.
5. Select **Enable the Printer Device**.
6. Set up the application server as described in either “Setting Up Windows NT4 Servers” or “Setting Up Windows 2000/2003 Servers” .

Setting Up Windows NT4 Servers

1. Navigate to **Control Panel | Network | Services** and ensure that the Microsoft TCP/IP Printing service is installed. If it is not, install it using the Microsoft installation instructions.
2. Add the thin client as the LPD printer by completing the following:
   a. Navigate to **Control Panel | Printers | Add Printers | My Computer | Add Port** and double-click **LPR PORT** (if you do not see **LPR Port**, ensure that the Microsoft TCP/IP Printing service is installed correctly).

b. Type the thin client IP address or DNS name in the **Name or address of host providing LPD** box.

c. Type the printer name (assigned in “Configuring LPD Services”) in the **Name of printer on that machine** box.

d. Click **OK**, and then click **NEXT**.

3. After you have selected the printer, you can perform your normal printer setup for the application server. For example, select the manufacturer printer type and printer name.

Setting Up Windows 2000/2003 Servers

1. Navigate to **Control Panel | Administrative Tools | Services** and ensure the Microsoft TCP/IP Printing service is installed. If it is not, install it using the Microsoft installation instructions.
2. Add the thin client as the LPD printer by completing the following:

a. Navigate to **Control Panel | Printers | Add Printers | Local Printer | Create a new port** and select **LPR PORT**.

Note

If you do not see LPR Port, ensure that the Microsoft TCP/IP Printing service is installed correctly.

b. Type the thin client IP address or DNS name in the **Name or address of host providing LPD** box.

c. Type the printer name (assigned in “Configuring LPD Services”) in the **Name of printer on that machine** box.

d. Click **OK**, and then click **NEXT**.

3. After you have selected the printer, you can perform your normal printer setup for the application server. For example, select the manufacturer printer type and printer name.

Configuring Touch Screens

The Touch Screen Setup allows configuration of touch screens that are connected to the thin client (USB and Serial). The Touch Screen Setup window is automatically invoked when the terminal detects that a touch screen is attached through a USB port and the setup (or calibration) has not been performed. In addition, the calibration sequence is executed whenever **Touch Screen** is selected from the Desktop menu.

Note

The Touch Screen desktop menu item is grayed out until a touch screen is connected. All ELO USB-based touch monitors and the M150-USB touch monitor from MicroTouch are supported.

The Touch Setup window prompts you to touch two circles on the screen to make the necessary calibration adjustment. Once calibrated, the adjustment values are saved in the local terminal NVRAM until the system is reset to factory default, or another type of touch monitor is connected.

This page intentionally blank.

4 Using and Configuring Access Connections

This chapter provides information and detailed instructions on using and configuring connections to access the enterprise server environment available to the thin client.

This section includes information on:

- “Using Ethernet Direct Access”
- “Using Wireless Direct Access”
- “Configuring PPPoE Access”
- “Configuring Dialup Modem Access”
- “Configuring PPTP VPN Access”

Using Ethernet Direct Access

This is a direct connection from the thin client Ethernet port to the enterprise intranet. No additional hardware is required.

Using Wireless Direct Access

An 802.11b USB Wireless Adapter can be used to access the enterprise intranet. The adapter connects to a USB port on the thin client and uses short-range wide-band radio to communicate with a wireless access point. Typically, wireless access points are located at several locations in the enterprise within range of the 802.11b USB Wireless Adapters and directly connect to the enterprise intranet.

After a wireless connection is made to the enterprise intranet, operation of the thin client through the wireless link is the same as Ethernet direct access.

Note

The speed of the connection is a function of signal strength, with a maximum of 11 Mbps.

For setup information, refer to "Setting Up Wireless Access."

Configuring PPPoE Access

PPPoE (Point-to-Point Protocol over Ethernet) is a specification for connecting users on an Ethernet to the Internet or intranet through a common broadband medium, such as a single DSL line, wireless device, or cable modem. PPPoE combines the Point-to-Point Protocol (PPP), commonly used in dialup connections, with the Ethernet protocol, which supports multiple users in a local area network. The PPP protocol information is encapsulated within an Ethernet frame.

The PPPoE Manager is available from the desktop to configure and invoke PPPoE connection to WAN. Once connected, all WAN packets are though a PPP connection over Ethernet to the DSL modem. The PPPoE Manager is not accessible for users with sign-on privilege set to None.

Selecting **PPPoE Manager** in the Desktop menu opens the PPPoE Manager dialog box. The PPPoE Manager dialog box can also be set to open automatically on thin client start as described in "Configuring Network Settings."

Figure 25 PPPoE Manager

Use the following guidelines:

- **Login Username** - Enter the login username required for this connection (up to 43 characters).
- **Login Password** - Enter the login password required for this connection (up to 15 characters).
- **Auto-connect on system startup** - When selected, causes the connection to be made automatically on system startup (default is cleared).
- **Use default gateway on remote (PPPoE) network** - When selected, causes the connection to use the default gateway (default is cleared).

After configuring the dialog box, click **Connect** to initiate a PPPoE connection.

Configuring Dialup Modem Access

A USB dial-up modem or a USB-to-Serial adapter connected to a serial modem can be used with the thin client to access a dial-up server.

The dial-up server may provide either of two paths to the enterprise intranet:

- An enterprise dial-up server will directly connect to the enterprise intranet.
- An Internet Service Provider (ISP) dial-up server provides access to the Internet, from which the thin client must access an enterprise PPTP VPN server that connects to the enterprise intranet.

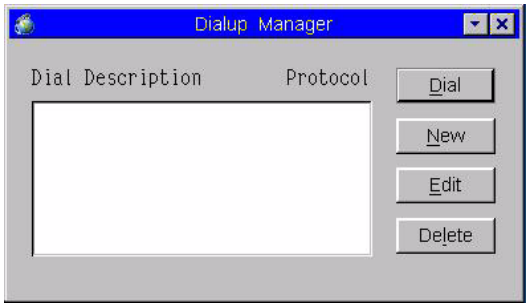
The Dialup Manager is used to initiate a connection to a dialup server through a modem.

Selecting **Dialup Manager** in the Desktop menu opens the Dialup Manager dialog box. The Dialup Manager dialog box can also be set to open automatically on thin client start as described in "Configuring Network Settings."

Note

Applications accessed through a dialup connection generally should have the **Optimize for low speed link** option selected in the user profile or the Connection Settings (ICA or RDP) dialog box.

Figure 26 Dialup Manager



Use the following guidelines:

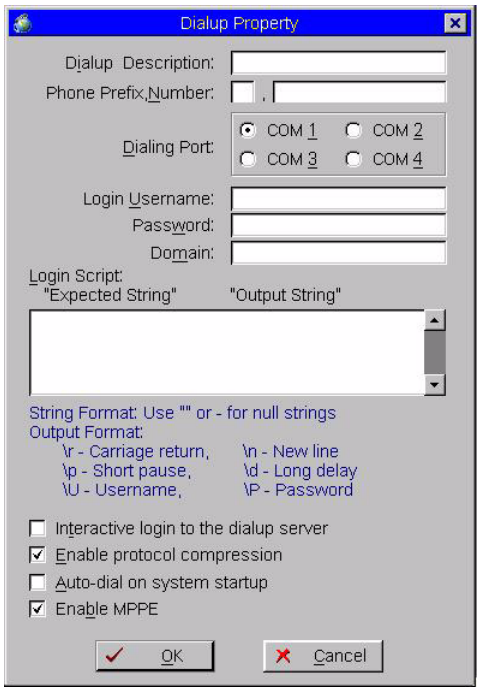
- **Dial Description/Protocol** area - Lists a description and protocol of each dialup property entry created using the Dialup Property dialog box.
- **Dial** - Initiates dialing for a currently-selected list entry. After initiation, a Dialup Status dialog box opens displaying messages and allowing you to refresh, reset, or disconnect the connection. If you are using a USB modem, the Serial Setup dialog box must be configured correctly to initiate a successful connection.
- **New** - Opens the Dialup Property dialog box. Use this dialog box to create a new connection entry in the list of connections.
- **Edit** - Opens the Dialup Property dialog box for a currently-selected list entry. Use this dialog box to edit the connection.
- **Delete** - Deletes the dialup property record for a currently-selected list entry. A warning is displayed, asking you to confirm the deletion.

Caution

Deleting the record is irreversible. A deleted record must be recreated to be made available again.

Dialup parameters for each dialing entry are entered using the Dialup Property dialog box.

Figure 27 Dialup Property



Use the following guidelines:

- **Dialup Description** - Enter the descriptive name that will appear in the Dialup Manager list of entries.
- **Phone Prefix Number** - Enter the phone number to be dialed.
- **Dialing Port** - Select the port through which this connection is to be made. The default is COM 1. For information on serial port configuration, refer to "Configuring Serial Communications."
- **Login Username**, **Password**, and **Domain** - Enter the login name, password, and domain required for this connection. This information is used for logging in to the PPP session.
- **Login Script** area - This feature provides a facility for logging in to systems which do not dedicate modem ports to the PPP protocol and require a serial login before initiating the PPP protocol (typically *NIX systems). It provides for automation of responses that otherwise must be entered manually in response to messages received from the dialed server and displayed in the message box of the Dialup Status dialog box. The specific scripts are unique to each target system. Using the escape codes listed under the box, as needed, create the script as **Expected String** <space> **Output String** pairs. Place quotation marks around strings that have spaces in them. The required strings can be tested by entering them manually in the dialup progress dialog box.

Note

Ask your network administrator for specific script requirements.

- **Interface login to the dialup server** - This option is an alternative to providing a login script. Enable (select) the interactive login feature only if the dialed server requires it. The dialup status dialog box (which opens when the connection is dialed) will display prompts from the dialed machine. Type the appropriate responses directly in the status display area.

Note

Ask your network administrator for the dialed server password and other dialog requirements.

- **Enable protocol compression** - When selected, allows data that is being communicated using the selected protocol (PPP or SLIP) to be compressed (default is selected).
- **Auto-dial on system startup** - When selected, causes the connection to be dialed automatically on system startup. (default is cleared).

Note

When the **Default Gateway**, **DNS Domain**, **DNS Server**, and **File Server** boxes in the Network Setup dialog box are configured and **Auto-dial on system startup** is enabled, both firmware revision checking and thin client sign-on are active (sign-on is only active if the profile on the FTP server enables it).

The **Default Gateway**, **DNS Domain**, **DNS Server**, and **File Server** boxes are required to enable access to an FTP server after the completion of establishing a PPP connection. However, only the File Server path is required to accomplish firmware revision checking and update (the more complicated the network topology in the target network, the more values are required in order to contact the FTP server).

If both Auto-dial on system startup is selected and Auto-connect on system startup is selected in a PPTP connection, the dial-up connection will be completed before the PPTP connection is initiated.

- **Enable MPPE** - When selected, enables MPPE (Microsoft Point-to-Point Encryption). MPPE is a method of encrypting data transferred across Point-to-Point Protocol (PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections. MPPE uses the RSA algorithm for encryption and supports 40-bit and 128-bit session keys, which are changed frequently to ensure security. MPPE does not compress or expand data.

After dialup initiation, the Dialup Status dialog box opens displaying messages and allowing you to refresh, reset, or disconnect the connection.

Figure 28 Dialup Status

Use the following guidelines:

- **Message area** - Displays messages as dialing progresses and the connection is established. If this is an interactive login connection, type appropriate responses to messages if you are prompted (ask your network administrator for the dialed server password and other dialog requirements).
- Data area - Displays data and statistics about the connection.
- **Refresh** - Updates the statistics display of the connection.
- **Reset** - Cancels dialing and resets the connection statistics area to 0.
- **Disconnect** - Disconnects the connection.

Configuring PPTP VPN Access

PPTP (Point-to-Point Tunneling Protocol) is a network protocol that enables the secure transfer of data between a remote client (in this case a thin client) and an enterprise server environment by creating a virtual private network (VPN) across TCP/IP-based data networks such as the Internet. It provides a password-protected path through the enterprise firewall to the enterprise server environment in which the network and session services required by thin clients reside.

The PPTP Manager dialog box is used to initiate a connection to a virtual private network (VPN) PPTP server through any of several access services (for example, dial-up, cable, or DSL). Connection parameters are entered using the PPTP Property dialog box.

Note

Modem access to an Internet Service Provider (ISP) server must be established before attempting to use this dialog box.

Selecting **PPTP Manager** in the Desktop menu opens the Dialup Manager dialog box. The PPTP Manager dialog box can also be set to open automatically on thin client start as described in "Configuring Network Settings."

Figure 29 PPTP Manager

Use the following guidelines:

- **Description/Protocol** area - Lists a description and protocol of each PPTP property entry created using the PPTP Property dialog box.
- **Connect** - Initiates a PPTP connection for a currently-selected list entry. After initiation, a PPTP Status dialog box opens (if **Show progress in detail** is selected in the PPTP Property dialog box and a path to an enterprise PPTP VPN server is available) displaying messages and allowing you to refresh or disconnect the connection. A PPTP connection is also initiated automatically on system start-up if this feature is selected in the PPTP Property dialog box.

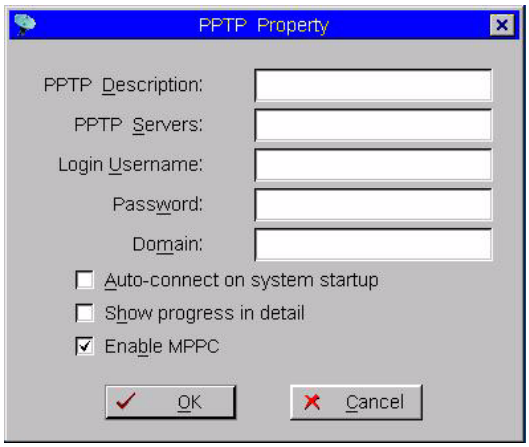
- **New** - Opens the PPTP Property dialog box. Use this dialog box to create a new connection entry in the list of connections.
- **Edit** - Opens the PPTP Property dialog box for a currently-selected list entry. Use this dialog box to edit the connection.
- **Delete** - Deletes the PPTP property record for a currently-selected list entry. A warning is displayed, asking you to confirm the deletion.

Caution

Deleting the record is irreversible. A deleted record must be recreated to be made available again.

PPTP parameters for each PPTP entry are entered using the PPTP Property dialog box.

Figure 30 PPTP Property

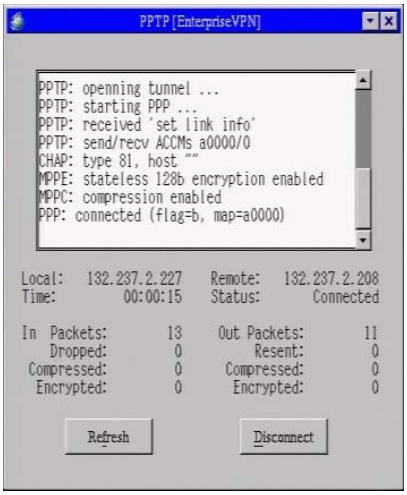


Use the following guidelines:

- **PPTP Description** - Enter the descriptive name that will appear in the PPTP Manager list of entries.
- **PPTP Servers** - List of IP addresses or host names with optional TCP port number of PPTP servers. Each entry with optional port number is specified as Name-or-IP:port, where :port is optional; if not specified, port 80 is used.
- **Login Username**, **Password**, **and Domain** - Enter the login name, password, and domain required for this connection.
- **Auto-connect on system startup** - When selected, causes the connection to be made automatically on system startup. (default is cleared).
- **Show progress in detail** - When selected, enables a PPTP Status dialog box opens (after connection initiation and a path to an enterprise PPTP VPN server is available) displaying messages and allowing you to refresh or disconnect the connection.
- **Enable MPPC** - When selected, enables Microsoft Point-to-Point Compression. The MPPC scheme is a means of representing arbitrary Point-to-Point Protocol (PPP) packets in a compressed form. The MPPC algorithm is designed to optimize processor utilization and bandwidth utilization in order to support a large number of simultaneous connections. The MPPC algorithm is also optimized to work efficiently in typical PPP scenarios (1500 byte MTU, and so on).

After connection initiation, the PPTP Status dialog box opens displaying messages and allowing you to refresh or disconnect the connection.

Figure 31 PPTP Status



Use the following guidelines:

- **Message area** - Displays messages as the connection is established. If this is an interactive login connection, type appropriate responses to messages if you are prompted (ask your network administrator for the PPTP server password and other dialog requirements).
- **Data area** - Displays data and statistics about the connection.
- **Refresh** - Updates the statistics display of the connection.
- **Disconnect** - Disconnects the connection.

5 Using the Network Test Tools

This chapter contains information on using the Network test tools available on the thin client.

Ping (Packet InterNet Groper) and Trace Route can be used for checking the integrity of the network connection (ping also checks the usability of the network configuration and the availability of all equipment required to communicate between the thin client and the ping destination). These tools can be accessed from the Network Test submenu of the Desktop menu (generally, ping and Trace Route are used for system diagnostics by, or under the direction of, a network administrator).

Using Ping

The ping dialog box executes the ping diagnostic utility and displays response messages. Ping is a diagnostic tool that sends an echo request to a network host. The host parameter is either a valid host name or an IP address. If the host is operational and on the network, it responds to the echo request. By default, echo requests are sent until interrupted (by clicking **Stop** in the ping dialog box). The ping utility sends one echo request per second and calculates round trip times and packet loss statistics, and displays a brief summary upon completion of the calculation.

The ping utility can be used to:

- Determine the status of the network and various foreign hosts
- Track and isolate hardware and software problems
- Test, measure, and manage networks
- Determine the IP address of a host if only the hostname is known

Note

Not all network equipment will respond to ping packets, since this is a common mechanism used in denial-of-service attacks. Lack of response does not necessarily indicate that the target of the ping is unusable for other purposes.

Figure 32 ping

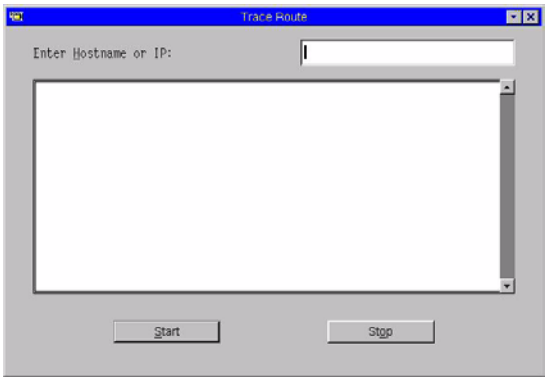
Use the following guidelines:

- **Enter Hostname or IP** - Enter the IP address, DNS-registered host name, or WINS-registered host name of the target to be pinged.
- Data area - Displays ping response messages. The ping command sends one echo request per second, calculates round trip times and packet loss statistics, and displays a brief summary upon completing the calculation.
- **Start** - Executes the ping command. If the host is operational and on the network, it responds to the echo request. By default, echo requests are sent until interrupted by clicking **Stop**.
- **Stop** - Terminates the ping request and leaves the ping dialog box open (so you can read the summary posted in the data area).

Using Trace Route

The Trace Route dialog box executes the tracert diagnostic utility and displays response messages. The tracert utility traces the path from your thin client to a network host. The host parameter is either a valid host name or an IP address. The tracert utility sends out a packet of information three times to each device (routers and computers) in the path and displays the round trip response times and identifying information in the message box.

Figure 33 Trace Route



Use the following guidelines:

- **Enter Hostname or IP** - Enter the IP address, DNS-registered host name, or WINS-registered host name of the target to be traced.
- Data area - Displays round-trip response time and identifying information for each device in the path.
- **Start** - Executes the tracert command.
- **Stop** - Terminates the tracert command and leaves the Trace Route dialog box open (so you can read the information posted in the data area).

Figures

Tables

Users Guide

Wyse® Winterm™ 1 series, Based on Wyse Thin OS
Issue: 121906

Written and published by:
Wyse Technology Inc., December 2006

Created using FrameMaker® and Acrobat®